



# Sanctuary Setup Guide

Sanctuary Application & Device Control v4.3.2

## 02\_102\_4.3.2.55

Lumension Security  
15880 North Greenway Hayden Loop, Suite 100  
Scottsdale, AZ 85260  
Phone: 480.970.1025  
Fax: 480.970.6323  
www.lumension.com

**Copyright © 1997-2008 Lumension Security® Inc. ALL RIGHTS RESERVED. U.S. Patent No. 6,990,660, Other Patents Pending.** This manual, as well as the software described in it, is furnished under license. No part of this manual may be reproduced, stored in a retrieval system, or transmitted in any form—electronic, mechanical, recording, or otherwise—except as permitted by such license.

**LIMIT OF LIABILITY/DISCLAIMER OF WARRANTY:** LUMENSION® CORPORATION MAKES NO REPRESENTATIONS OR WARRANTIES IN REGARDS TO THE ACCURACY OR COMPLETENESS OF THE INFORMATION PROVIDED IN THIS MANUAL. LUMENSION® CORPORATION RESERVES THE RIGHT TO MAKE CHANGES TO THE INFORMATION DESCRIBED IN THIS MANUAL AT ANY TIME WITHOUT NOTICE AND WITHOUT OBLIGATION TO NOTIFY ANY PERSON OF SUCH CHANGES. THE INFORMATION PROVIDED IN THE MANUAL IS NOT GUARANTEED OR WARRANTED TO PRODUCE ANY PARTICULAR RESULT, AND THE ADVICE AND STRATEGIES CONTAINED MAY NOT BE SUITABLE FOR EVERY ORGANIZATION. NO WARRANTY MAY BE CREATED OR EXTENDED WITH RESPECT TO THIS MANUAL BY SALES REPRESENTATIVES OR WRITTEN SALES MATERIALS. LUMENSION® CORPORATION SHALL NOT BE LIABLE FOR ANY LOSS OF PROFIT OR ANY OTHER DAMAGES ARISING FROM THE USE OF THIS MANUAL, INCLUDING BUT NOT LIMITED TO SPECIAL, INCIDENTAL, CONSEQUENTIAL, OR OTHER DAMAGES

### Trademarks:

Lumension® Corporation, Sanctuary™, Sanctuary Application Control Suite™, Sanctuary, Sanctuary Application Control Custom Edition™, securing the enterprise™, Sanctuary Application Control™, Sanctuary Application Control Server Edition™, Sanctuary Application Control™, Sanctuary for Embedded Devices™, Sanctuary Application Control Terminal Services Edition™, and their associated logos are registered trademarks or trademarks of Lumension® Corporation.



RSA Secured® is a registered trademark of RSA Security Inc.

Apache is a trademark of the Apache Software Foundation

In addition, other companies' names and products mentioned in this document, if any, may be either registered trademarks or trademarks of their respective owners.

### Feedback:

Your feedback lets us know if we are meeting your documentation needs. E-mail the Lumension Technical Publications department at [techpubs@Lumension.com](mailto:techpubs@Lumension.com) to tell us what you like best, what you like least, and to report any inaccuracies.



# Table of Contents

About This Guide .....	xi
Document Conventions .....	xiii
Contacting Lumension Security .....	xiv
Lumension Security Corporate Offices .....	xiv
Product Pricing .....	xv
Lumension Security Sales and Support .....	xvi

## Chapter 1: Installing Sanctuary's Components \_\_\_\_\_ 1

Sanctuary Architecture .....	1
To Install Sanctuary Products .....	3
Ghost Image Deployment .....	5
Transport Layer Security .....	6
Using TLS for Client-Sanctuary Application Server Communication .....	7
Using TLS for the Inter-Sanctuary Application Server Communication .....	10
What is a Digital Certificate? .....	12
What is a Certificate Authority? .....	13
Basic Security Rules .....	13
CD/DVD Burning .....	13
The Boot Sequence .....	13
Hard Disk Encryption .....	14
The Seal/Chassis Intrusion Protector .....	14
Password Protect the BIOS .....	14
Administrative Rights .....	14
Power Users .....	15
Access Policy .....	15
NTFS Partition (Mandatory to Install our Product) .....	15
Recovery Console .....	15
Safe Mode .....	15
Service Packs and Hot Fixes .....	15
Firewalls .....	16
Password Policies .....	16
Access Policy .....	16
Private and Public Key Generation .....	16

## Chapter 2: Installing the Sanctuary Database \_\_\_\_\_ 17

Choosing a SQL Engine .....	17
Before you Install .....	18
Stage 1: To Install the SQL Database Engine .....	19
Stage 2: To Install the Sanctuary Database .....	20
Database Clustering .....	24



- What is Database Clustering? ..... 24
  - Terminology ..... 25
  - Requirements ..... 25
  - To Implement a Database Cluster ..... 26
- Items Created During the Sanctuary Database Setup ..... 28
- Chapter 3: Using the Key Pair Generator ..... 29**
  - Introduction ..... 29
  - Starting the Key Pair Generator ..... 30
  - Generating a Key Pair ..... 30
  - Deploying the Key Pair ..... 31
- Chapter 4: Installing the Sanctuary Application Server ..... 33**
  - Before you Install ..... 33
  - To Install the Sanctuary Application Control ..... 36
  - Items Created During Sanctuary Application Server Setup ..... 52
- Chapter 5: Installing the Sanctuary Management Console ..... 53**
  - Before you Install ..... 53
  - To Install the Sanctuary Management Console ..... 54
  - Items Created During Sanctuary Management Console Setup ..... 60
- Chapter 6: Installing the Sanctuary Client on Your Endpoint Computers 61**
  - System Requirements ..... 61
    - Overall System Requirements ..... 61
    - Client Computer Requirements ..... 62
  - To Install Sanctuary Clients ..... 63
  - Unattended Installation of the Sanctuary Client ..... 79
  - Uninstalling the Sanctuary Client ..... 79
  - Load Balancing Methods ..... 81
    - What is Load Balancing ..... 81
    - How Does Round Robin DNS Works? ..... 81
    - Advantages of DNS Round Robin ..... 81
  - Items Created During the Sanctuary Client Setup ..... 83
- Chapter 7: The Sanctuary Authorization Service Tool ..... 85**
  - What is the Sanctuary Authorization Service Tool? ..... 85
  - To Install the Sanctuary Authorization Service Tool ..... 86
  - Configuring WSUS ..... 91



**Chapter 8: Unattended Client Installation \_\_\_\_\_ 93**

What is an MSI File? .....	95
Creating a Transform File (MST) for an Existing MSI File .....	95
Prerequisites for Creating a Sanctuary Client Deployment Tool Package .....	95
To Install the Sanctuary Client Deployment Tool .....	96
To Install Packages .....	97
To Install the Sanctuary Client: MST File Generation .....	97
Using the Sanctuary Client Deployment Tool to Install the Sanctuary Client .....	106
Using the Command Line to Install Clients .....	117
Using Windows Group Policy to Install Clients .....	118
Querying the Client Status .....	124
Sanctuary Client Deployment Tool Menus .....	124
Packages Menu .....	124
Computers Menu .....	126
Help Menu .....	128
Context Menus .....	128
The Options Screen .....	130

**Chapter 9: Using the SXDomain Command Line Tool \_\_\_\_\_ 133**

Introduction .....	133
The SXDomain Parameters .....	133
Examples .....	134
Scheduling Domain Synchronizations .....	135

**Chapter 10: Registering your Sanctuary Product \_\_\_\_\_ 141**

Licensing .....	141
Obtaining a License .....	141
Evaluation License .....	141
Full License .....	142
License File Location .....	142
License File Format .....	142
License-Related Sanctuary Application Server Actions at Start-Up .....	144
License-Related Sanctuary Application Server Actions While Running .....	144
License-Related Client Actions .....	144

**Appendix A: Detailed System Requirements and Limitations \_\_\_\_\_ 147**

System Requirements .....	147
Sanctuary Device Control .....	151
Terminal Services Limitations .....	151
The RunAs Command Limitations .....	152



**Appendix B: Registry Keys \_\_\_\_\_ 153**

Sanctuary Application Server Registry Keys ..... 153

Database Connection Loss Registry Keys ..... 153

Log Insertion Process Registry Keys ..... 154

Debugging Registry Keys ..... 155

General Registry Keys ..... 156

Security Registry Keys ..... 157

Sanctuary Client Registry Keys ..... 163

Sanctuary Management Console ..... 166

**Appendix C: Upgrading from Old Versions \_\_\_\_\_ 167**

Sanctuary Device Control ..... 168

Sanctuary Server Edition ..... 169

Upgrading Server-side Components ..... 169

Upgrading from a Previous Sanctuary Application Server Version ..... 170

Upgrading Guideline ..... 173

**Appendix D: Installing Sanctuary Components on Windows XP/2003/Vista  
175**

Connection Between Sanctuary Application Server and the Sanctuary Database ..... 175

Connection Between the Sanctuary Management Console and the Sanctuary Application  
Server ..... 176

Stage 1: Configuring a Fixed Port on the Server ..... 176

Stage 2: Opening the Port on the Server Firewall ..... 177

Connecting to the Server Using the Fixed Port ..... 177

Connecting Using the Endpoint Mapper ..... 177

Summary ..... 179

Connection between the Sanctuary Client and the Sanctuary Application Server ..... 179

Configuring the Firewall ..... 179

**Appendix E: Opening Firewall Ports for Client Deployment \_\_\_\_\_ 181**

To Manually Open the Ports on a Computer-by-Computer Basis ..... 181

To Open the Ports on a Computer-by-Computer Basis with a .bat File ..... 182

To open the Firewall Ports via an Active Directory Group policy ..... 182

    To Create the Group Policy (GPO) ..... 183

    To Improve Security ..... 186

**Appendix F: Using the Synchronization Script for Novell \_\_\_\_\_ 187**

Introduction ..... 187

What Components are Required? ..... 187

How does the Novell Interface Works? ..... 188

Synchronization Script Parameters ..... 188



How to use Novell's Synchronization Script .....	189
Script Examples .....	190
What Can go Wrong and How do I Fix It? .....	190
Installing your Synchronization Script .....	191

## **Appendix G: Using Novell Shares for your DataFileDirectory \_\_\_\_\_ 195**

DataFileDirectory Access to a Novell Share .....	195
Transparent Sanctuary Application Server authentication for Novell eDirectory .....	195

## **Appendix H: Installing a Certificate Authority for Encryption and TLS Commu- nication \_\_\_\_\_ 203**

Requirements .....	203
Integrating DNS with Active Directory .....	203
Installing the Certificate Services .....	204
Checking Certificates are Correctly Issued to the Users .....	210
Checking Certificates are Correctly Issued to Endpoint Machines .....	214

## **Appendix I: Controlling Administrative Rights for Sanctuary's Administrators 215**

Ctrlacx.vbs .....	215
Requirements .....	215
Usage .....	216
Examples .....	216
What to do After Running the Script .....	217

## **Appendix J: Installation Checklist \_\_\_\_\_ 221**

Requirements .....	221
If you are Using Windows... ..	221
If you are Using Novell... ..	221
The Sanctuary Database .....	221
Software .....	221
Hardware .....	221
Network Configuration .....	222
Additional Settings .....	222
Firewall Configuration .....	222
The Sanctuary Application Server .....	222
Software .....	222
Hardware .....	222
The Sanctuary Management Console .....	222
Firewall Configuration .....	223



- Sanctuary Client ..... 223
  - Software ..... 223
  - Hardware ..... 223
  - Network Configuration ..... 223
  - Additional Settings ..... 224
  - Firewall Configuration ..... 224
- License ..... 224
  - Private and Public Keys ..... 224
- Data file directory ..... 224
- SXS Account ..... 225
- Certificate Authority ..... 225
- Implementation Actions ..... 225
- Installation checklist ..... 227
- Defining Permissions in Sanctuary Device Control ..... 231

**Appendix K: Installing Sanctuary Application Control Terminal Services Edition** \_\_\_\_\_ **237**

- Introducing Sanctuary Application Control Terminal Services Edition ..... 237
- Installing the Server Side Components ..... 237
- Installing the Sanctuary Client ..... 238
  - The Installation Procedure ..... 238
- Uninstalling the Sanctuary Client ..... 242

**Appendix L: Installing Sanctuary in Windows XP Embedded** \_\_\_\_\_ **243**

- What is Windows XP Embedded ..... 243
- Thin Clients ..... 243
  - Available Shells ..... 244
- What does Windows XP Embedded does not Include ..... 244
- Installing Sanctuary in Windows XP Embedded ..... 245
  - What Server Side Components you Need ..... 245
  - What Client Components you Need ..... 245
  - Componentized the Sanctuary Client ..... 247
- Functionalities and Devices Supported by Sanctuary in Windows XP Embedded ..... 248
- How to Configure the Client ..... 251
  - Sanctuary Application Server (SXS) ..... 251
  - Encrypted Communications ..... 252
- How to Update Policies ..... 253
- Enhance Write Filter (EWF) ..... 255
  - Sanctuary Client & EWF ..... 256
- Minimum Requirements ..... 256
- Known Issues ..... 256

**Appendix M: Glossary** \_\_\_\_\_ **259**





**Appendix N: Index** 

---

 **265**





# Preface

This guide explains in detail how to install all components of your Sanctuary solution. For a quick introduction on how to test and understand the way Sanctuary works and protects your organization, consult the Sanctuary Quick Setup Guide.

## About This Guide

---

This guide contains the following chapters and appendices:

- [Chapter 1, “Installing Sanctuary’s Components”](#) shows you the basic Sanctuary architecture, security tips, and guides you through the process of installing the Sanctuary components.
- [Chapter 2, “Installing the Sanctuary Database”](#) explains how to set up the database needed by Sanctuary.
- [Chapter 4, “Installing the Sanctuary Application Server”](#) explains how to set up the component that serves as a link between the Sanctuary client and the database and/or the management console and the database.
- [Chapter 5, “Installing the Sanctuary Management Console”](#) explains how to set up the console used to administer Sanctuary.
- [Chapter 3, “Using the Key Pair Generator”](#) explains how to generate public and private keys before you deploy the Sanctuary Client to the machines you want to protect.
- [Chapter 6, “Installing the Sanctuary Client on Your Endpoint Computers”](#) guides you on how to set up the Sanctuary Client on the computers that will be protected by Sanctuary.
- [Chapter 7, “The Sanctuary Authorization Service Tool”](#) explains the setup procedures for the SUS/WSUS (Software Update Services & Windows Server Update Services) update partner tool used for our Sanctuary Application Control Suite programs (Sanctuary Application Control, Sanctuary Application Control Server Edition, or Sanctuary Application Control Terminal Services Edition).
- [Chapter 8, “Unattended Client Installation”](#) shows you how to deploy clients silently.
- [Chapter 9, “Using the SXDomain Command Line Tool”](#) explains how to synchronize information between the Sanctuary Database and the domain controller.
- [Chapter 10, “Registering your Sanctuary Product ”](#) explains the Sanctuary licensing model.
- [Appendix A, “Detailed System Requirements and Limitations”](#) details the hardware and software you need for an optimum operation of the software.
- [Appendix B, “Registry Keys”](#) provides detailed information about registry key settings for servers and clients.
- [Appendix C, “Upgrading from Old Versions”](#) explains how to upgrade from a previous version of Sanctuary Device Control and Sanctuary Application Control Suite.
- [Appendix D, “Installing Sanctuary Components on Windows XP/2003/Vista”](#) explains how to configure this system to work with Sanctuary programs.
- [Appendix E, “Opening Firewall Ports for Client Deployment”](#) covers how to open the required ports needed for the client deployment technique described in [Chapter 8, “Unattended Client Installation”](#).



- [Appendix F, “Using the Synchronization Script for Novell”](#) provides a quick setup guide for synchronizing Novell eDirectory objects to define device/application permissions.
- [Appendix G, “Using Novell Shares for your DataFileDirectory”](#) undertakes the task of explaining how to set the data file directory (DataFileDirectory or DFD) in your Novell server.
- [Appendix H, “Installing a Certificate Authority for Encryption and TLS Communication”](#) describes how to install a Microsoft Certificate Authority needed for client-Sanctuary Application Server and intra-Sanctuary Application Server TLS communication. This authority is also needed if you plan to centrally encrypt removable devices (if using Sanctuary Device Control).
- [Appendix I, “Controlling Administrative Rights for Sanctuary’s Administrators”](#) describes a file script used to set and control the rights to administer Organizational Units/Users/Computers/Groups in Active Directory.
- [Appendix J, “Installation Checklist”](#) contains several tables to guide you through the initial setup process.
- [Appendix K, “Installing Sanctuary Application Control Terminal Services Edition”](#) introduces Sanctuary for Terminals Services.
- [Appendix L, “Installing Sanctuary in Windows XP Embedded ”](#) discusses how to configure and install Sanctuary on Windows Embedded systems.
- The [“Glossary”](#) provides definitions of standard terms used throughout the guide.
- The [“Index”](#) provides quick access to information, items, or topics.

Some of these chapters are only relevant for some programs of our product suite.



**Note:** Each chapter has an introduction paragraph explaining to which part of our suite they correspond.



**Tip:** Lumension documentation is updated on a regular basis. To acquire the latest version of this document, please refer to the Lumension Support Documentation Web site ([www.lumension.com/support/documentation.html](http://www.lumension.com/support/documentation.html)).

## Document Conventions




The following conventions are used throughout Lumension documentation to help you identify various information types:

### Document Conventions

Convention	Usage
<b>bold</b>	Command names, database names, options, wizard names, window and screen objects (i.e. Click the <b>OK</b> button)
<i>italics</i>	New terms, variables, and window and page names
UPPERCASE	SQL commands and keyboard keys
monospace	File names, path names, programs, executables, command syntax, and property names

The icons used throughout Lumension documentation identify the following types of information:

### Icons Used

Icon	Alert Label	Description
	<b>Note:</b>	Identifies paragraphs that contain notes or recommendations.
	<b>Tip:</b>	Identifies paragraphs that contain tips, shortcuts, or other helpful product information.
	<b>Warning:</b>	Identifies paragraphs that contain vital instructions, cautions or critical information.



---

## Contacting Lumension Security

---

### Lumension Security Corporate Offices

#### Global Headquarters

15880 North Greenway Hayden Loop, Suite 100  
Scottsdale, AZ 85260  
United States of America  
Phone: +1 480.970.1025  
Fax: +1 480.970.6323  
E-mail: [info@lumension.com](mailto:info@lumension.com)

#### Florida Office

2290 West Eau Gallie  
Suite 212  
Melbourne, FL 32935  
Fax: +1 321 751 6454

#### United Kingdom Office

Unit C1, Windsor Place  
Faraday Road, Crawley  
West Sussex, London RH10 9TF  
United Kingdom  
Phone: +44 (0)1293 558 880  
Fax: +44 (0)1293 558 881  
E-mail: [patchlink.emea@lumension.com](mailto:patchlink.emea@lumension.com)

#### European Headquarters

Atrium Business Park  
Z.A. Bourmicht  
23 rue du Puits Romain  
L-8070 Bertrange, Luxembourg  
Phone: +352 265 364 11  
Fax: +352 265 364 12

#### Hong Kong Office

18/F, One International Finance Centre  
1 Harbour View Street, Central, Hong Kong  
Phone: +852 2166 8145  
Fax: +852 2166 8999  
E-mail: [patchlink.apac@lumension.com](mailto:patchlink.apac@lumension.com)

#### Australia Office

Level 20, Tower II, Darling Park  
201 Sussex Street  
Sydney, NSW  
Australia 2000  
Phone: +61 2 9006 1654  
Fax: +61 2 9006 1010  
E-mail: [patchlink.apac@lumension.com](mailto:patchlink.apac@lumension.com)



### **Spain Office**

Paseo de la Castellana, 141 pl.20 ed. Cusco IV  
28046 Madrid  
Spain  
Phone: +34 91 749 80 40  
Fax: +34 91 570 71 99  
E-mail: [patchlink.emea@lumension.com](mailto:patchlink.emea@lumension.com)

### **Singapore Office**

Level 27, Prudential Tower  
30 Cecil Street  
Singapore 049712  
Phone: +65 6725 6415  
Fax: +65 6725 6363  
E-mail: [patchlink.apac@lumension.com](mailto:patchlink.apac@lumension.com)

### **India Office**

51 Kalpataru Court  
Dr. C.G. Road  
Behind R.K. Studio, Chembur  
Mumbai 400 074  
India  
Phone: +91 22 6515 5403  
E-mail: [patchlink.apac@lumension.com](mailto:patchlink.apac@lumension.com)

### **US Federal Solutions Group**

Virginia Office - Federal Solutions Group  
13755 Sunrise Valley Drive, Suite 203  
Herndon, VA 20171, USA  
Phone: +1 443 889 3291  
Fax: +1 301 441 2212  
E-mail: [patchlink.federalsales@lumension.com](mailto:patchlink.federalsales@lumension.com)

## **Product Pricing**

To receive pricing and licensing information, please visit the [Lumension: How Do I Purchase?](http://www.lumension.com/purchase/purchase_form.html)  
( [http://www.lumension.com/purchase/purchase\\_form.html](http://www.lumension.com/purchase/purchase_form.html) ) Web page or contact the  
Lumension Sales Department.



## Lumension Security Sales and Support

### North America Sales

Phone: +1 480.970.1025 (Option 1)

E-mail: [sales@lumension.com](mailto:sales@lumension.com)

### International Sales

Phone: +1 480.970.1025 (Option 1)

E-mail: [internationalsales@lumension.com](mailto:internationalsales@lumension.com)

### PatchLink Technical Support

Phone: +1 480.970.1025 (Option 2)

+44 (0) 1908 357 897 (United Kingdom)

+61 (02) 8223 9810 (Australia)

+852 3071 4690 (Hong Kong)

+65 6622 1078 (Singapore)

E-mail: [patchlink.support@lumension.com](mailto:patchlink.support@lumension.com)

[patchlink.apac.support@lumension.com](mailto:patchlink.apac.support@lumension.com) (APAC)

[patchlink.emea.support@lumension.com](mailto:patchlink.emea.support@lumension.com) (EMEA)

### Sanctuary Technical Support

Phone: +352 265 364 300

+1 877 713 8600 (US Toll Free)

+44 800 012 1869 (UK Toll Free)

E-mail: [sanctuary.support@lumension.com](mailto:sanctuary.support@lumension.com)

### Business Partnerships

Phone: +1 480 444 1681

E-Mail: [patchlink.businessdevelopment@lumension.com](mailto:patchlink.businessdevelopment@lumension.com)

### Professional Services

Phone: +1 480 663 8702

E-mail: [patchlink.professionalservices@lumension.com](mailto:patchlink.professionalservices@lumension.com)





# 1 Installing Sanctuary's Components

The information in this chapter is relevant to all Sanctuary products.

This chapter guides you through the procedure for installing the various Sanctuary components. You can find a complete description of the Sanctuary products in the corresponding User Guide.

## Sanctuary Architecture

---

A Sanctuary solution includes the following four main components (for a full description see your User Guide):

- One Sanctuary Database — This serves as the central repository of authorization information (devices/applications).
- One or more Sanctuary Application Server with one or (optionally) more Data File Directory (DFD) — This is used to communicate between the Sanctuary Database and the protected clients.
- The Sanctuary Client — installed on each computer you want to protect. You will also need to install the Sanctuary Client on the same computer where the Sanctuary Management Console is installed if you want to encrypt removable devices; authorize DVDs/CDs (see next point).
- Administrative tools — including the Sanctuary Management Console. This provides the administrative interface to the Sanctuary Application Server. This interface, which can be installed on one or more computers, is used to configure the solution and perform a range of day-to-day administrative tasks. You can install the console on one of the servers you are using for the Sanctuary Database or the Sanctuary Application Server or on any computer that has access to the Sanctuary Application Server.

An implementation can have more than one *Sanctuary Application Server* connected over a wide area to one *Sanctuary Database*. This means that Sanctuary can provide a resilient and scalable solution to your security issues.



The relationship between the Sanctuary components is represented in the following figure:

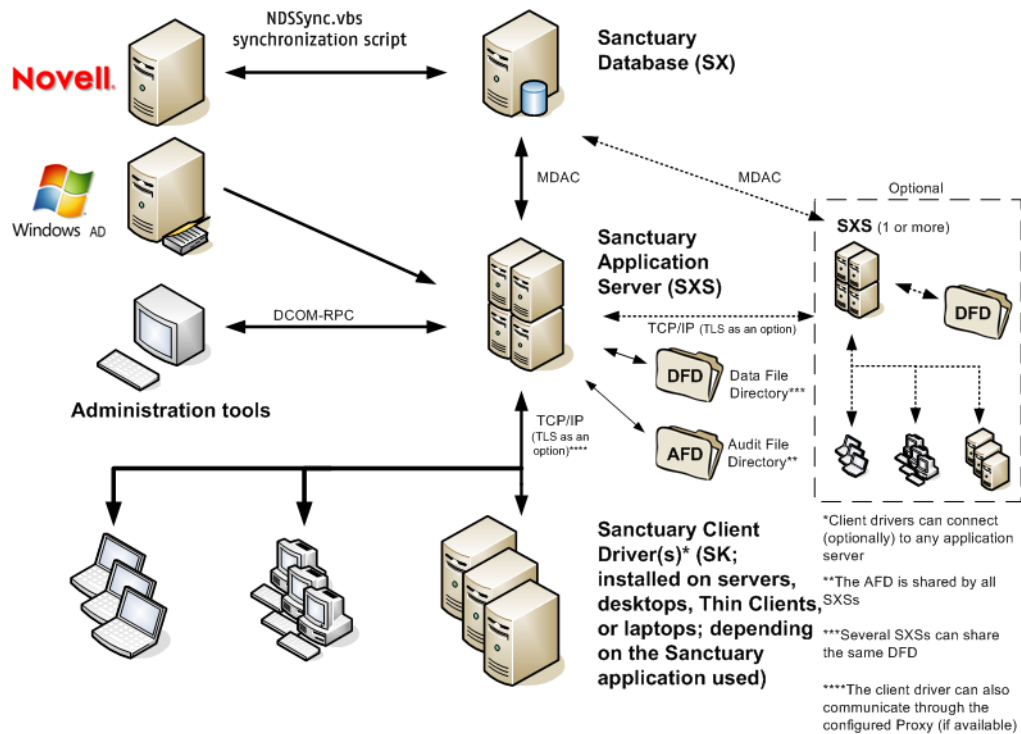


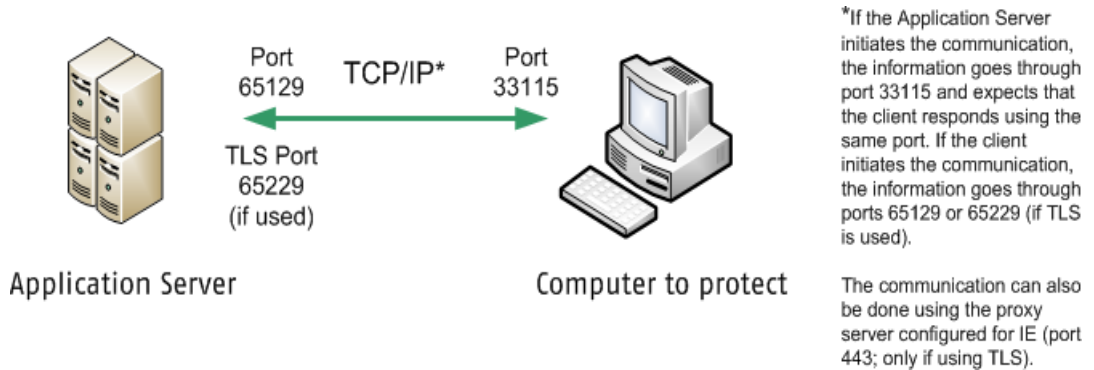
Figure 1.1 Sanctuary's architecture



**Note:** We do not describe the installation of Microsoft SQL Server in replication mode in this guide.



**Note:** We assume that the TCP/IP protocol is configured properly ((network card working, protocol installed, IP address and mask defined, DNS and Gateway configured, machine in domain and with correct name; consults Windows' help file) and the proper ports opened (65129 on the server side and 33115 on the computer used as a client; as shown in the following image) and the proper ports opened prior to the installation.



**Figure 1.2** Sanctuary's TCP/IP configuration

## To Install Sanctuary Products

Although Sanctuary Software is an extremely powerful security solution, its setup is straightforward. The installation routine can be broken down into the following stages:

1. **Decide whether you are going to use an extra encryption layer** for Sanctuary Client - Sanctuary Application Server and intra-Sanctuary Application Server communications or not. If you decide to use it, you need to install a Certificate Authority. This is also needed if you want to centrally encrypt removable media using *Sanctuary Device Control*. See [“Transport Layer Security”](#) on page 6, [Appendix H, “Installing a Certificate Authority for Encryption and TLS Communication”](#) on page 203, and *Sanctuary Device Control User Guide*.
2. Install the Sanctuary Database on the computer that is to hold authorization information for devices and/or executables, scripts and macros. You can find a detailed installation procedure explanation in [Chapter 2, “Installing the Sanctuary Database”](#) on page 17.
3. **Generate the key pair** that is used to sign/encrypt messages/media. See [Chapter 3, “Using the Key Pair Generator”](#) on page 29.
4. Install the Sanctuary Application Server on the computer or computers that serve as intermediates between the Sanctuary Client and the Sanctuary Database, distributing the list of device/software permissions for each client computer and/or User/group. See [Chapter 4, “Installing the Sanctuary Application Server”](#) on page 33.
5. Install the Sanctuary Management Console on the computer(s) you are going to use to configure Sanctuary, and subsequently carry out your day-to-day administrative tasks and procedures. See [Chapter 5, “Installing the Sanctuary Management Console”](#) on page 53.
6. Install a Sanctuary Client **and test the predefined permissions for devices and/or executables, scripts or macros**. You can install the client on the same machine that you are using for the



*Sanctuary Database*, *Sanctuary Application Server*, and *Sanctuary Management Console* (some limitations apply). See [Chapter 6, “Installing the Sanctuary Client on Your Endpoint Computers”](#) on page 61.

7. **Define some test permissions** for devices and/or executable files using the console installed on step 3 and test these on the client machine. See the *Quick Setup Guide*.
8. **Define company's policies** (permissions, rules, and settings). Determining and defining which users get access to which devices and/or executables, scripts and macros. This step is done before installing or rolling out any clients. Installing Sanctuary Clients without a good policy definition would result in a loss of productivity. Consult the *Sanctuary Application Control Control Suite User Guide* and/or *Sanctuary Device ControlSanctuary User Guide* for more information.
9. **Plan the client installation strategy and deploy your clients** in production machines to begin enjoying immediately the benefits of being protected by Sanctuary. See [Chapter 8, “Unattended Client Installation”](#) on page 93.
10. **Define a synchronization schema** to be used for your Microsoft Domains or Novell eDirectory structure. See [Chapter 9, “Using the SXDomain Command Line Tool”](#) on page 133.

You can find a detailed explanation of the functions carried out by the various Sanctuary administration components in the *Sanctuary Application Control Suite User Guide* and/or *Sanctuary Device Control User Guide*. We recommend that you read these through thoroughly before starting the implement Sanctuary products.

At any time after installing the *Sanctuary Database*, *Sanctuary Application Server*, *Sanctuary Management Console*, or the *Sanctuary Client* you can modify or uninstall the components by running their respective setup.exe files.

If any setup routine stops, (e.g. if a severe error is encountered or if it is canceled by user request) the routine attempts to clean up and roll back any modifications it made to your computer. It also produces log files containing the reason why the setup failed. These are placed in %TMP% directory (of the user account who is doing the installation) and named sxdbi.log, setupcltsu.log, setupsmc.log, setupdb.log, and setupsxs.log. If your setup fails, and you make a support call to Lumension, you will be asked to send these files to help us diagnose the problem.



**Warning:** You should resolve all hardware conflicts before installing Sanctuary solutions. You can use Windows' Device Manager to troubleshoot and fix software-configurable devices. All hardware devices that use jumper pins or dip switches must be configured manually.



**Warning:** It is critical to determine the Policy Definition that is best for your organization. This is where you define which users get access to which devices and/or executables. This step must be done before any clients are installed or rolled out. If you install clients without a good policy definition, this will result in a loss of efficiency or it could prevent users from accessing their devices. **Define policies BEFORE installing any clients!.**

## Ghost Image Deployment

A common problem that administrators face is how to deploy a 'standard' computer to a new user or when upgrading to new hardware. They normally do this by installing all necessary software on a 'fresh' computer and then use 'Ghost' software to create an image of it. The administrator then imprints this image on all new computers.

The Sanctuary Client can be included in the 'ghost' image. You can do this, using the following steps:

1. Install the Sanctuary Client on the machine to be 'ghosted', as you would do on any other client computer.
2. Disable the Client Hardening mode (if active; see your *User's Manual*)
3. Change all drivers to start on demand mode. To do this, use Regedit to modify the following values found in  
HKLM\System\CurrentControlSet\Services\  
scomc: Start, REG\_DWORD = 4  
sk: Start, REG\_DWORD = 4  
sk-ndis: Start, REG\_DWORD = 4
4. Disable the *SKNDIS* filter from the TCP/IP properties (*Network Connections* from the *Start* menu)
5. Delete the value in reference to *sxd-vdd.dll* in the registry:  
HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\  
Control\VirtualDeviceDrivers
6. Remove the *rtnotify* entry from the registry key (note the path to add it back when deploying the ghost image):  
HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\  
CurrentVersion\Run
7. Reboot the computer. The driver is installed but does not run.
8. Proceed to create the Ghost image from this 'standard' computer.



When deploying the Ghost image:

1. Change the SID (which uniquely identifies the computer) and the name of the computer. This can be done using Ghostwalker or the freeware SIDchanger tool available from the SYSinternals website (<http://technet.microsoft.com/en-us/sysinternals/default.aspx>).
2. Change the starting mode of each driver back to its original state. To do this, use *Regedit* to modify the following values found in:  
HKLM\System\CurrentControlSet\Services\  
scomc: Start, REG\_DWORD = 2  
sk: Start, REG\_DWORD = 0  
sk-ndis: Start, REG\_DWORD = 3
3. Add in the registry key:  
HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\  
Control\VirtualDeviceDrivers  
the following value:  
%SYSTEMROOT%\System32\sxd-vdd.dll
4. Add back *rtnotify* entry to the registry key:  
HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\  
CurrentVersion\Run
5. Reboot the 'new' computer.
6. Activate the *SKNDIS* filter from the TCP/IP properties (*Network Connections* from the *Start* menu).

## Transport Layer Security

---

The Transport Layer Security (TLS) protocol (based on SSL — Secure Socket Layers) addresses security issues related to message interception during communication between hosts. The deployment of TLS, client and server side, is the primary defense against compromised clients or mixed networks where it is possible to intercept transmitted messages.

TLS has specific advantages when addressing message security issues:

- The identities of peers can be authenticated using asymmetric or public key cryptography, allowing the safe exchange of encrypted information, coupled with a Certificate Authority (see [Appendix H, "Installing a Certificate Authority for Encryption and TLS Communication"](#)). Clients can verify that the IP address and name are consistent with the DNS records, inhibiting 'man in the middle' and DNS 'spoofing' exploits.
- Message's contents cannot be modified while en route between two TLS negotiated hosts. Either party has the ability of detecting TLS protocol violations.

However, there are also some disadvantages to using the TLS protocol:



- Cryptography, specifically when it involves public key operations, is CPU-intensive and using TLS may result in a performance loss. The level of performance loss depends on factors such as your environment, the total number of permissions required, if you want to use shadowing or not, and so on. Unfortunately, it is impossible to know beforehand how large the performance loss will be for your particular organization.
- A TLS environment requires maintenance — the system administrator must configure the system and manage certificates.

You should consider carefully whether your organization needs this extra security, i.e. if your company either uses sensitive data or has to meet certain security regulations.

## Using TLS for Client-Sanctuary Application Server Communication

There are two ways in which a Sanctuary Client can communicate with a Sanctuary Application Server. It can use:

- A *Pull operation* in which the client establishes a connection with the server to:
  - Obtain the most recent permission updates.
  - Upload its log files.
  - Upload its shadow files.

If using TLS protocol, the authentication and confidentiality of the data exchanged is always guaranteed.

- A *Push operation*:
  - In a first case, the Sanctuary Application Server establishes a connection with the client to request it to:
    - Perform a scan.
    - Upload its log file
    - Upload its shadow files.
    - Contact the server to receive the latest permission updates
  - In a second case the Sanctuary Application Server ‘Pings’ the client to update its client list or begin another communication or process.

Push messages are very limited and basic and therefore do not use TLS. Sanctuary Application Server sends a short message informing the client to callback with an ID number, nothing else. This message, although not encrypted, is signed. The Sanctuary Client then opens a connection channel with the Sanctuary Application Server — either using TLS or not, as defined when installed — and sends back the ID number. The Sanctuary Application Server(s) verify that there is a pending request for this communication and instruct the client what to do next.

The callback message (see also [Chapter 1, “Using TLS for the Inter-Sanctuary Application Server Communication”](#) on page 10) is authenticated using the private/public key pair, which must be generated before installing the Sanctuary Application Server. Messages are always signed with the server private key and clients use the corresponding public key to guarantee that the messages come from genuine servers.



Since the messages exchanged with the server do not contain confidential data, there is no need to encrypt them, i.e. using TLS for push messages would not provide any significant benefits.

When the communication mode used is TLS, the Sanctuary Client:

- Checks that the size of the package received is at least big enough to hold the server signature, rejecting any packages smaller than this minimum size.
- Rejects packages that are bigger than the maximum allowed size.
- Verifies the signature and integrity of the message, for the packages that have been accepted.

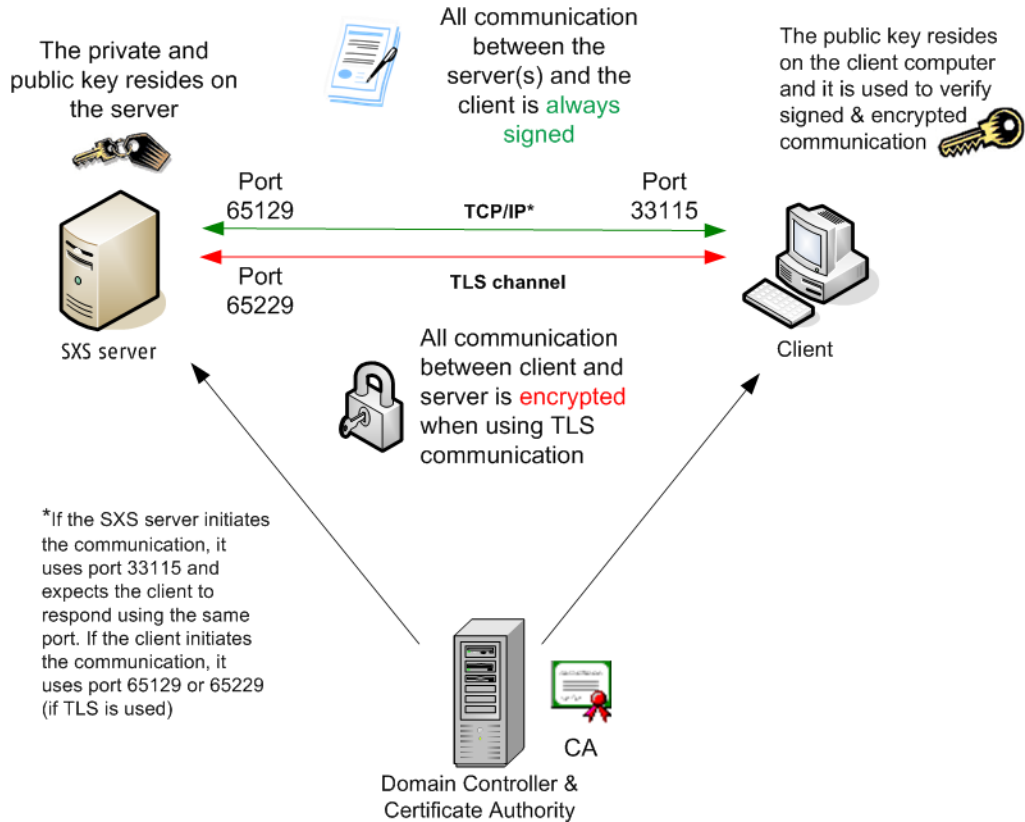
When a client receives a valid Sanctuary Application Server command, it begins sending back the requested data through a TLS connection (if configured). This data can comprise:

- Scan results.
- Log files.
- Shadow files.
- Permission updates.





- 'Ping' information.



**Figure 1.3** Sanctuary Client: Using the TLS protocol for client-Sanctuary Application Server communication



If the program does not auto-generate the required certificate (by attempting to obtain it from the Certificate Authority) you can either try to import it or generate it with the Wizard. You must ensure that it is signed by a private key as shown in the following image:

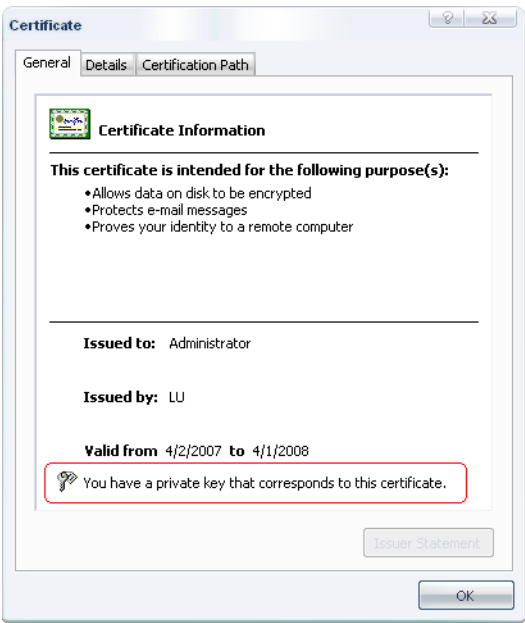


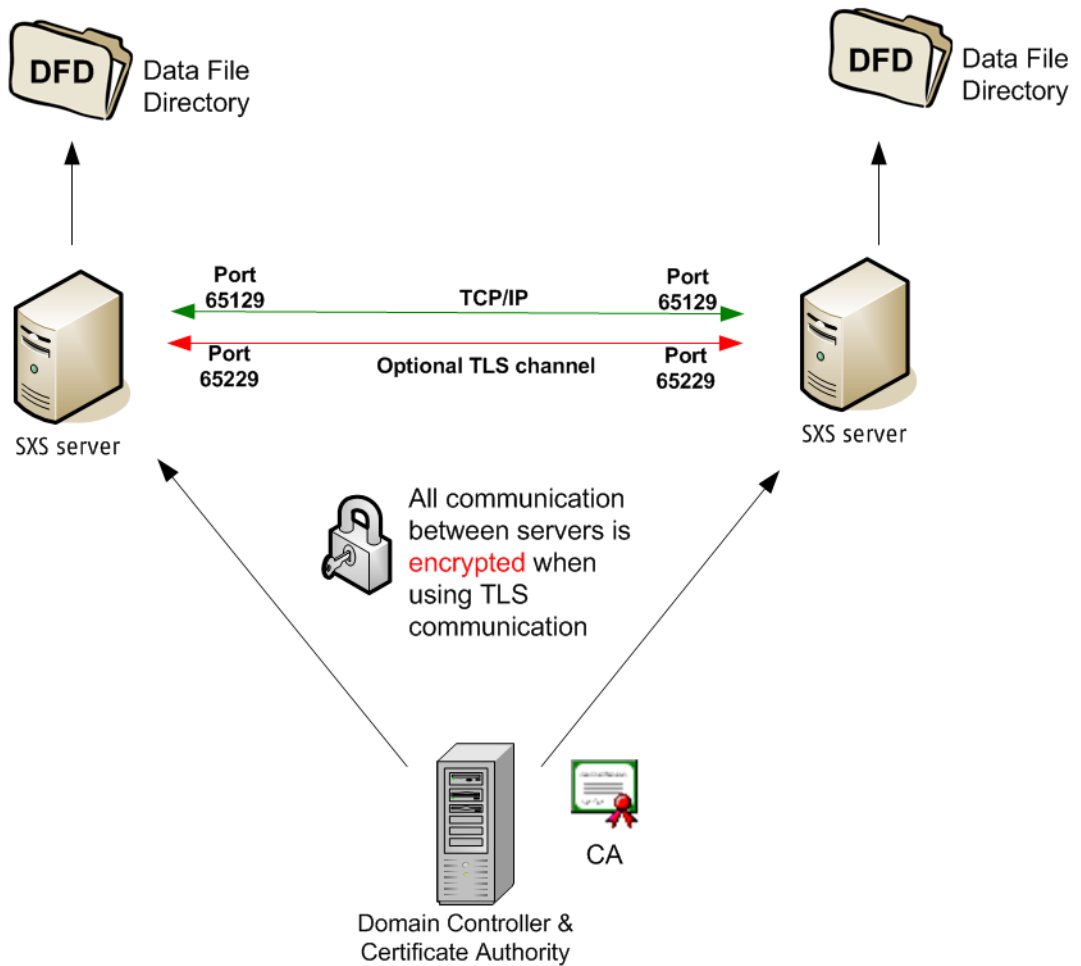
Figure 1.4 Signed certificate

## Using TLS for the Inter-Sanctuary Application Server Communication

If your Sanctuary implementation contains several Sanctuary Application Servers and uses distributed Data File Directories (DFD), then since confidential information is exchanged between these, it is a good idea to choose to use the TLS protocol when installing them. For example, if you



plan to define read/write shadow rules (see the *Sanctuary Device Control User Guide* for a complete explanation), there could be a constant flow of shadowed files circulating between them. Using the TLS protocol option assures that data is encrypted.



**Figure 1.5** Sanctuary Application Server: Using the TLS protocol for intra-Sanctuary Application Server communication

Sanctuary Application Server machines may have multiple DNS names and multiple certificates. The certificate selected by Sanctuary Application Server must match the DNS name used by the Sanctuary Client and other Sanctuary Application Servers when they communicate over secure TLS



ports. These values can be manually overridden by modifying a registry key (see [Chapter B, “Sanctuary Application Server registry keys \(security registry keys\)”](#) on page 157 for more information).

The value in 'ServerName' can be used to specify a fully qualified DNS name that Sanctuary Application Servers register in the servers table and communicate to clients in callbacks. The value 'ServerCertSerial' is used to specify the serial number of the certificate that Sanctuary Application Server should use for TLS communication. The format of this value is *exactly* the same as the one that Sanctuary Application Server displays when a certificate is loaded, for example, 3738DCAE0003000001C0. (The MMC Certificates snap-in uses almost the same format, except it has blanks after every two digits. These blanks must NOT be specified for the Sanctuary Application Server value.)

Server callback messages (see also [Chapter 1, “Using TLS for Client-Sanctuary Application Server Communication”](#) on page 7) include the server's DNS name and port number(s). This ensures that the client only answers the particular contacting Sanctuary Application Server even if the client has no prior information about it. The message also includes a timestamp, which prevents the client from replying to old requests.

### What is a Digital Certificate?

A digital certificate is an electronic presentation card that establishes your identity and credentials when doing transactions over a channel. Certificates are issued by a Certification Authority. They contain, among other things:

- A digital signature, indicating which certificate-issuing authority generated them. This lets a recipient verify that the certificate is genuine.
- A public key, to be used for encrypting messages and digital signatures. All messages encrypted using the public key can be decrypted using the corresponding private key pair (see a complete description on any of the Sanctuary user's guides).

Most certificates used today are based on the X.509 v3 certificate standard.

All messages encrypted using the public key can be decrypted using the corresponding private key pair (see a complete description on any of the Sanctuary user's guides).

Typically, certificates also contain the following information:

- Certificate's version and serial number.
- Signature algorithm.
- Validity (not before, not after).
- Authority and subject's ID.
- Digital signature of the issuer, testifying the validity of the binding between the subject's public key and the subject's identifier information.

## What is a Certificate Authority?

A Certificate Authority (CA) is an entity that issues and manages certificates in a network. As part of a public key infrastructure, a CA checks with a registration authority (RA) to verify the information provided by the requestor of a digital certificate. If the RA verifies the requestor's information, the CA can then issue a certificate stating that the public key contained in it belongs to the person, computer, or entity noted in the same certificate. The idea behind this security process is that the user trusts the CA and can verify its signature and can also corroborate that a certain public key belongs to whoever is identified in the certificate.

You either trust a CA or not. If you trust a CA, this means that you have confidence that it has proper policies in place when evaluating certificates requests. In addition to this, you also trust that the CA will revoke certificates that should no longer be considered as being valid, publishing an up-to-date CRL (Certification Revocation List).

## Basic Security Rules

---

This section lists a series of basic security rules that are highly recommended prior to deploying the Sanctuary Client on a production network.

### CD/DVD Burning

Windows' own CD/DVD recording capacity is controlled by a service called Image Mastering Applications Programming Interface (IMAPI; run by LocalSystem). You should not give R/W access to LocalSystem for the 'DVD/CD Drive' class or music CDs. If you do so and the service is running, then the user can create CD/DVD copies — using Windows Media Player, Windows Explorer, or any other program that uses this service — of any file from the hard disk, including private data, proprietary information, music, etc. See details in Sanctuary Device Control User Guide. Some third-party burning software do not need the IMAPI service and can be disabled.

### The Boot Sequence

Change the boot sequence so that the machine boots from the Hard Disk Drive first. If the Floppy or the DVD/CD-ROM is the first boot device, someone can use a bootable medium that can directly access the hard disk drive and quickly reset the administrator password.



**Note:** This does not apply for SCSI setups, since you can simply change the boot ID or LUN boot and bypass any boot sequence. Adaptec PCI BIOS are not password protected, but recent PC BIOS versions give you the extra choice to boot from a "SCSI DEVICE", overriding SCSI controller settings.



### Hard Disk Encryption

You can prevent unauthorized user access to a computer hard disk by using "off-line" techniques, such as using boot disks with other operating systems, encrypting the machine's disk(s) with third-party software. This also adds another security layer in the event a machine containing legally protected data is lost or stolen.

### The Seal/Chassis Intrusion Protector

Protect the hardware with a seal and/or chassis intrusion protection hardware. Otherwise, an intruder could obtain administrator level access to the system using an external boot device to bypass workstation security software.

### Password Protect the BIOS

Although this is important, its effectiveness is greatly reduced without chassis intrusion security (see previous point), since someone just needs to locate the CMOS reset jumper to gain access to data on the local hard drive.



**Note:** Some workstations have an intrusion trigger which is stored in the BIOS and displayed when the machine cover has been removed.

### Administrative Rights

Even though Sanctuary can enforce policies for local administrators and limit their ability to change or remove the Sanctuary Client through client hardening, users should *NEVER* be members of the local group called *Administrators*. If a user is the administrator of his own computer, then he has complete, unrestricted access to this computer. There are many ways to uninstall, disable, or change the configuration of programs and services (and time settings) when you are a local administrator. For example, one could delete files, registry keys, uninstall the product, delete the driver entries, and use the recovery console. In addition to this, viruses will execute using administrative privileges unless you are using a component of our Sanctuary Application Control Suite (Sanctuary Application Control, Sanctuary Application Control Server Edition, or Sanctuary Application Control Terminal Services Edition).

Consequently, it is **not** a good practice to grant the users administrative rights to their computers. It is impossible to control/manage a desktop when the user has local administrative rights (thus higher TCO). Nevertheless, some special programs require administrative rights to run properly. You can easily find tools that allow users to run programs with administrative rights only when needed. 'RunAs Professional' is one of them.



**Note:** Sanctuary's Client Hardening feature will protect Sanctuary's clients for a possible tamper even if the user is an administrator. See any of the Usre's Guides for more information.

## Power Users

Users who are members of the built-in 'Power Users' group are a special case which requires careful consideration. Power Users have elevated permissions and privileges on their local machines - depending on the operating system version - and can generally install and run applications, change permissions, customize settings, modify and create accounts, etc. This may give them an unwanted direct or indirect ability to bypass or tamper with standard Windows based system policies. Non-trusted users should never be members of the Power Users group, unless you secure the execution environment by using Sanctuary Application Control Suite.

## Access Policy

In general, you should have a network and file access policy as restrictive as possible including using only NTFS partitions. By default, you should deny all access and then, give access only when/if necessary.

## NTFS Partition (Mandatory to Install our Product)

NTFS (New Technology File System) is an update of the FAT32 (File Allocation Table), FAT12 (initial version of FAT), FAT16, and VFAT systems which, in turn, are also updates from the old MS-DOS FAT system. NTFS offers several security and performance enhancements and advantages over older file systems. Among them, we can quote a superior architecture, support for larger files, enhanced reliability, automatic encryption and decryption, disk quota tracking and limiting, change journals, disk defragmenter, sparse file support, and improved security and permissions when managing files.

## Recovery Console

The Recovery Console, which is available on the Windows DVD/CD-ROM or via a MSDN subscription, allows the user to disable any driver related to Sanctuary. However, this requires the local administrator password. This is one of the reasons why you should change the boot sequence as previously described. If you fail to do this, then a user may be able to boot the system using a different operating system bypassing system security. The user can, for example, boot from the CD with a Linux OS and manipulate the NTFS partitions to gain access to the stored data.

## Safe Mode

Safe mode boot causes no threat to Sanctuary drivers, which continue to run even when you boot in this mode.

## Service Packs and Hot Fixes

In general, you should always install the latest service packs and hot fixes for the operating system and the different applications you use.



### Firewalls

Traditional perimeter-based security systems, like firewalls, are complementary to the endpoint protection provided by Sanctuary Software.

### Password Policies

You should have a strong security policy, in particular regarding the choice of the passwords. You should refuse blank, short, and simple passwords, enforcing long and complex character sequences.

### Access Policy

In general, you should have an access policy as restrictive as possible (using NTFS, permissions, etc.). By default, deny all access, and then just give access if and when necessary.

### Private and Public Key Generation

You should deploy Sanctuary software in a production environment using a securely generated key pair. Use the KEYGEN.EXE tool that is included on your installation CD to create your own unique private and public key. The private key (sx-private.key) is literally the 'key' to the security that is provided by Sanctuary solutions. As with all private keys, extra diligence should be used to ensure its confidentiality.





## 2 Installing the Sanctuary Database

This chapter explains how to install the SQL Engine and *Sanctuary Database*. Whereas [Chapter 1, “Installing Sanctuary’s Components”](#) provides an overview of the entire setup, this chapter focuses exclusively on the database requirements. The information in this chapter is relevant to all Sanctuary software suite products.



**Warning:** Although you can use Windows XP, 2000 Pro, or Vista x 86 for the database or/and console, you cannot use it for the Sanctuary Application Server (or client component in the case of Sanctuary Application Control Server Edition). If you are planning to spread Sanctuary components among several machines, one of them in an XP operating system — database and/or management console —, you should read carefully [Appendix D, “Installing Sanctuary Components on Windows XP/2003/Vista”](#) on page 175 before proceeding.



**Warning:** If you are updating from a previous version of our software or have one of our products, you should always make a backup of your database before proceeding.

### Choosing a SQL Engine

The database used by Sanctuary software requires a Microsoft SQL Server database. This can be SQL Server 2000 SP4/2005 SP2 or SQL Server 2005 Express Edition SP2.

The database server you choose depends on the size of your implementation and which, if any, of these Microsoft SQL Server databases you are currently using within your organization.

SQL Server 2005 Express Edition is certainly sufficient for installations of up to 200 connected Sanctuary clients when you are using Sanctuary Device Control, or 50 Sanctuary clients when you are using Sanctuary Application Control Suite. Please note that there are inherent limits when using SQL Server 2005 Express Edition including:

- 4 GB Database size limit.
- No parallel processing of index operations.
- Only uses up to 1GB RAM.
- Only one CPU, no workload governor.
- No query analyzer.

SQL Server 2005 Express Edition may be an attractive option for sites that do not already use SQL Server. It is available free of charge, eliminating the expense of purchasing the SQL Server.



We recommend using a full-blown SQL Server at sites in which it is already installed. SQL Server should always be used for sites serving 200 or more connected Sanctuary clients.

See our online knowledgebase (at [www.Lumension.com](http://www.Lumension.com)) for advice about which Microsoft SQL Server database you should choose.

The Sanctuary Setup CD includes an installation of SQL Server 2005 Express Edition.



**Note:** You can start using SQL Server 2005 Express Edition, and migrate to SQL Server later, should this be necessary. You cannot create a cluster using SQL Server 2005 Express Edition.



**Note:** To successfully install SQL Server 2005 Express Edition you must already have Microsoft's .Net Framework 2.0 and Windows Installer 3.1 (or later) installed on your machine.



**Warning:** We strongly recommend downloading and applying the latest SQL Server service packs from [www.microsoft.com](http://www.microsoft.com) before putting the system in production. Make sure you download the appropriate file. For example, service packs for Microsoft SQL Server cannot be applied to a SQL Server 2005 Express Edition database.

### Before you Install

---

Before you start installing your database engine of choice, you must first check that the computer meets the minimum requirements. See [Appendix A, "Detailed System Requirements and Limitations"](#) on page 147 for details.



**Note:** You must activate the 'Server' service (File and Print Sharing to Microsoft Networks) before attempting to install SQL Server on your machine. This is particularly important for Novell users who do not necessary already have this service running on their machines.

## Stage 1: To Install the SQL Database Engine



**Note:** This procedure explains how to install SQL Server 2005 Express Edition. You can skip this stage if you already have SQL Server 2000 SP4/2005 SP2 running on the machine that you want to host the Sanctuary Database.

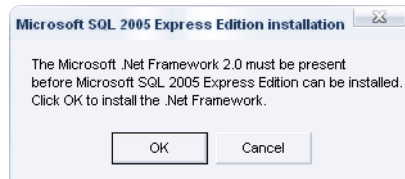
1. Log on to the computer on which you want to install the SQL Database engine. You must use an account with administrative rights.
2. Close all programs running on the computer.
3. Insert the Sanctuary CD in your DVD/CD drive and execute run.vbs located in the \SERVER\SQL2005 folder on the installation CD. The setup starts.



**Note:** You must have Microsoft Installer v3.1 or later installed on your system. The setup prompts you to install this if you do not have it.



**Note:** If you do not have Microsoft's .Net Framework v2.0 (or later) installed on your computer, the following dialog is displayed, Click on OK and follow the instructions to install .Net Framework v2.0 (or later).



**Figure 2.1** Installing SQL Server 2005 Express Edition, .Net not available

4. If you accept the terms of the license agreement, select the **“I accept the terms in the license agreement”** option and click on **Next**.
5. Click **INSTALL** to continue the installation.





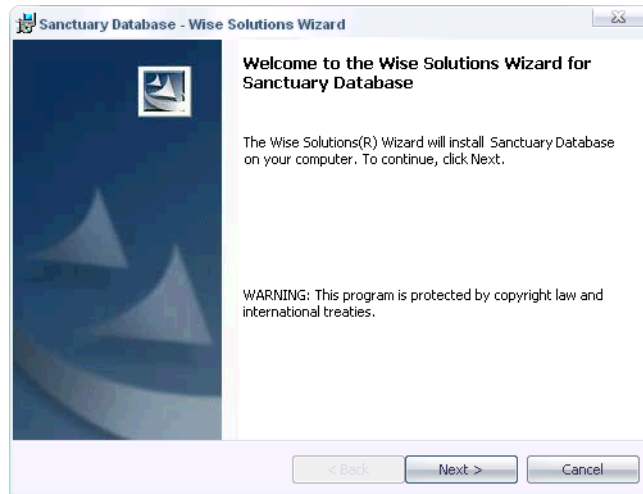
**Note:** Make sure that the TCP/IP protocol is enabled for your SQL database. You can use the 'SQL Server Configuration Manager' tool in the 'Start → Programs → Microsoft SQL Server 2005' menu to check or manage protocols.

### Stage 2: To Install the Sanctuary Database

---

The Sanctuary database component requires a Microsoft SQL Server database. This can be SQL Server 2000 SP4/2005 SP2 or SQL Server 2005 Express Edition. If a database server is found, the setup adds a single database called 'sx'.

1. Log on to the computer on which the SQL Server is running. The account you use must have:
  - Administrative rights.
  - Access to SQL Server.
2. Close all programs running on the computer.
3. Insert the Sanctuary CD in your DVD/CD and run SETUP.EXE located on the \SERVER\DB folder.
4. The *Welcome* dialog is displayed.



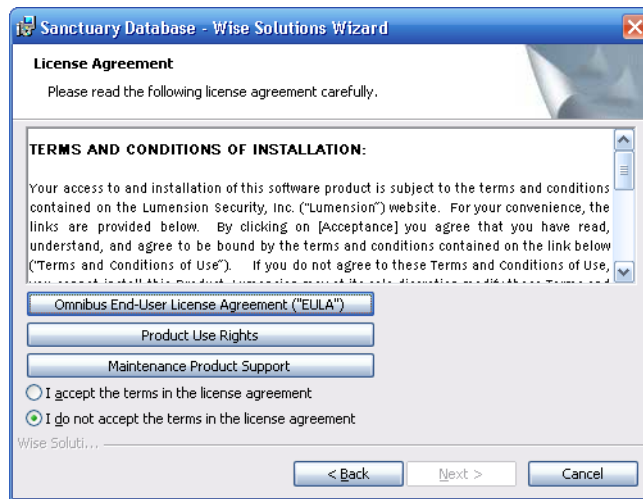
**Figure 2.2** Sanctuary Database installation: First step

5. Click on NEXT to continue.



**Warning:** The setup will not generate a log file if it is launched running the db.msi file instead of the setup.exe file. The log file may be important in case of troubleshooting and when contacting Lumension.

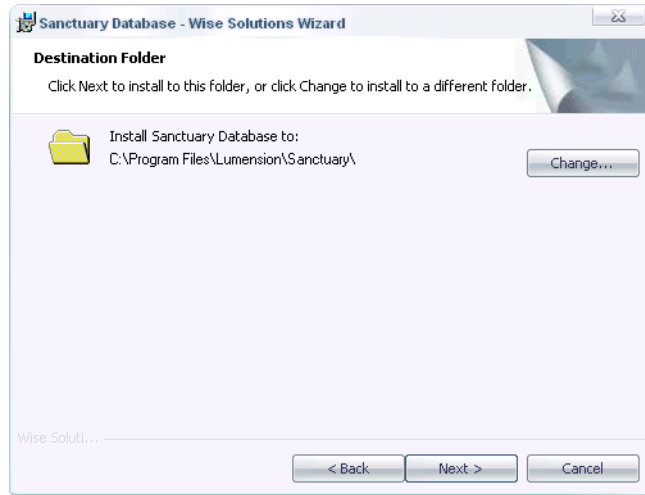
6. The next dialog displays the License Agreement.



**Figure 2.3** Sanctuary Database installation: License agreement



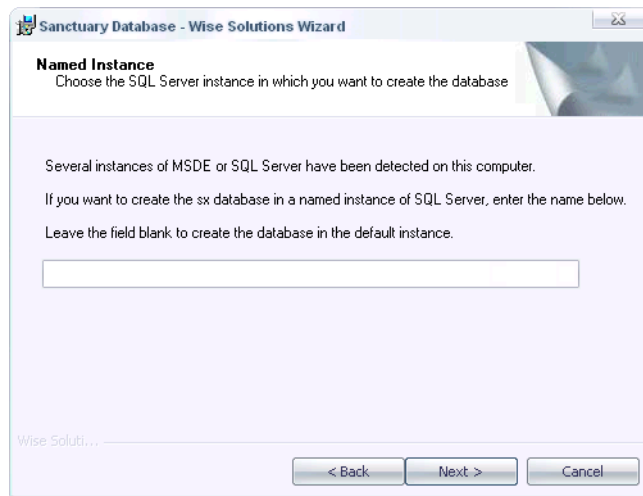
7. If you accept the terms of the license agreement, select the **“I accept the terms in the license agreement”** option and click on **Next**. You can also click on any of the three available buttons to read the license agreements.



**Figure 2.4** Sanctuary Database installation: Destination folder

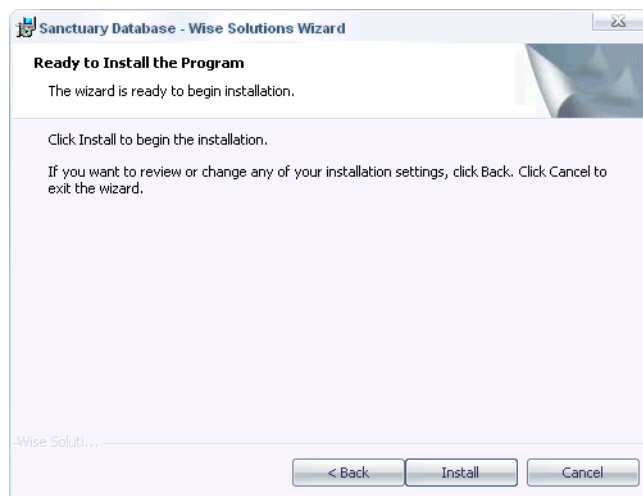
8. Choose the folder in which you want to create the Sanctuary Database and click on NEXT. By default, the database is installed in the C:\Program Files\Lumension Security\Sanctuary folder. To choose another location, click on CHANGE and browse to the folder you want.

If you already have several instances of the database engine on your computer, you are asked to select the one you want to use. You should use the `servername\instancename` format:



**Figure 2.5** Sanctuary Database installation: Select SQL instance

The setup wizard is ready to start the installation:

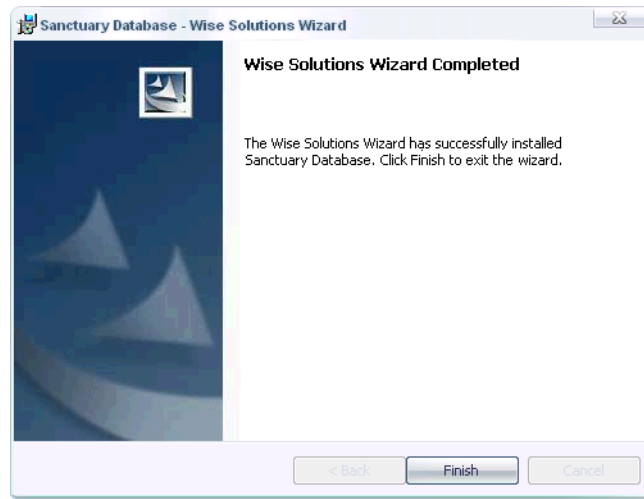


**Figure 2.6** Sanctuary Database installation: Final step



9. Click on the INSTALL button to perform the setup.

The SQL scripts run and the database is created. This process normally takes less than 2 minutes, depending on your hardware. Once completed, the final screen is displayed:



**Figure 2.7** Sanctuary Database installation: Ending the installation wizard

10. Click on FINISH to close the wizard.

## Database Clustering

---

The *Sanctuary Database* is the repository where all permissions and hashes (which define whether an application or device can be used or not) are stored. As an alternative to installing it on a single machine, you can choose to install Sanctuary Database on a clustered server to provide a fault-tolerant system, as described below. Once you have at least two servers in a cluster with SQL working, you can proceed to install the database as described in the previous procedure.

### What is Database Clustering?

A cluster is a group of computers, or nodes, which functions as a single system to provide high availability and fault tolerance. Database clustering is a failover technology. It ensures that the execution environment and services move to another computer in the cluster in case of a node failure, maximizing the database availability. (Database clustering does not provide scalability; It does not focus on performance or distributing the traffic to different servers.)



## Terminology

- **Cluster:** A group of computers configured to work together to serve clients in a similar fashion.
- **Node:** Each server participating in a cluster is called a node.
- **Maximum # of nodes in a cluster:** The maximum number of servers that can form a cluster. This is eight in Windows 2003 Enterprise, with at most 16 SQL instances.
- **Heartbeat:** The nodes in a cluster remain in constant communication through the exchange of periodic messages called heartbeats.
- **Virtual IP (VIP):** The client system communicates with the DB server using a virtual IP address. MSCS (Microsoft Cluster Service) takes care of redirecting the client request to the active server and hence the client does not have to worry about which server in a cluster is active.
- **MSCS (Microsoft Cluster Service):** A Windows component, which once installed through the Control Panel, guides you through the steps needed to create a cluster service (cluadmin.exe).
- **Quorum:** Physical disk where all configuration parameters are stocked. Without quorum the cluster cannot work — it must be a backup.
- **Failover:** Capability to switch, automatically or manually, to a standby computer in a cluster. In normal situations, one (primary or active) computer provides the service while a second one (failover) is present to run the services if the primary fails.
- **Failback:** Operation where a cluster is back and running after a failover. Control passes on to the active or primary computer of a cluster.



**Note:** The same operating system must be installed on the nodes of a cluster database server.

## Requirements

Database clustering requires:

- At least two servers (up to the maximum that the operating system used in the cluster supports).
- Two network adapters per server — one to communicate with clients, the other one to communicate between the nodes that form the cluster (heartbeat). If only two computers are used, you can join them using a simple cross-link cable.
- A Shared Disk Array, SAN, or SCSI device to host the database.
- Microsoft Cluster Service (MSCS) to form the cluster. This is provided with Windows Operating Systems.
- One instance of SQL Server 2000 SP4/2005 SP2, including a SQL server, SQL server agent, and Full text search service.



### To Implement a Database Cluster

1. Define the cluster using Microsoft Cluster Service (MSCS). To do this, you need to name the cluster, add nodes to it, configure the network interfaces to define those that are public and those that are private (heartbeat), and, finally, test the cluster configuration.

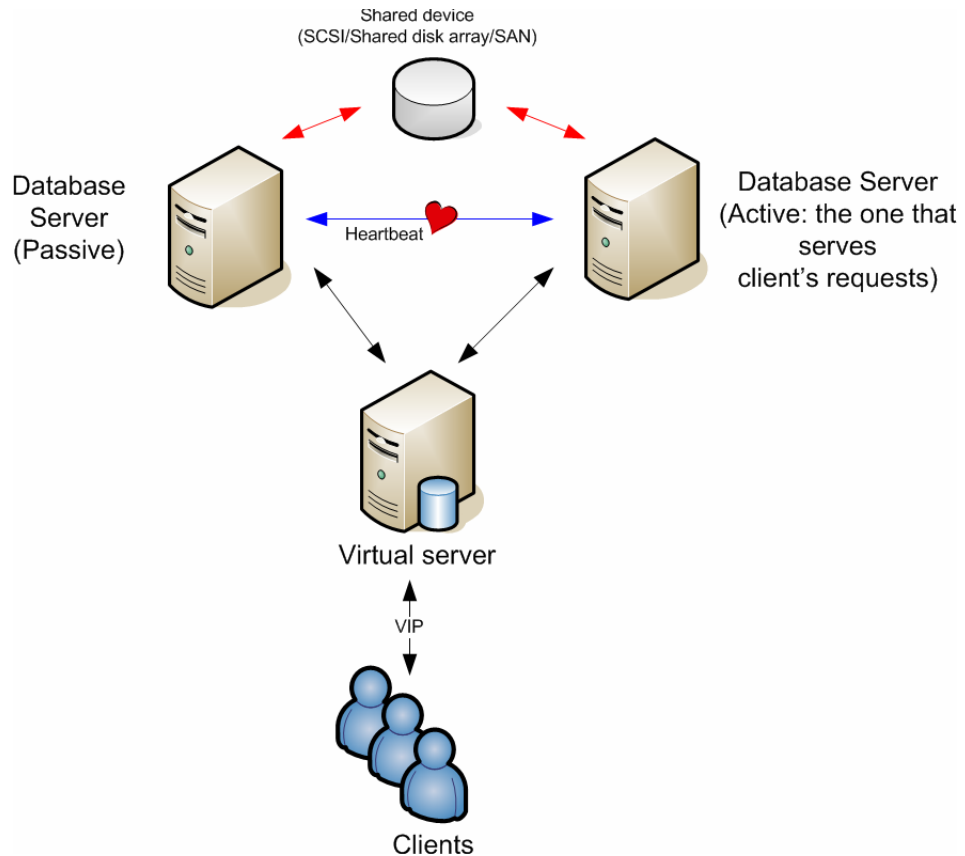
MSCS provides three cluster models:

- **Single node server cluster** — This does not provide failover. This model is mainly used to organize resources on a server for administrative conveyance.
- **Single quorum** — This is the traditional cluster model. It maintains the cluster configuration data on a single cluster storage device connected to all nodes. For n-node clusters, the cluster is active until the last node in a cluster is working. Data is stored on a single cluster storage device (SCSI etc.). Data synchronization is not required. We recommend that you use a RAID solution for the cluster storage devices.
- **Majority node set** — Each node maintains its own copy of the cluster configuration data (quorum). More than half the nodes in a cluster must be running to keep the cluster working. This configuration is useful if you need to host applications that can failover, but where there is another, application-specific way, to replicate or mirror data between nodes.

Note that in Single Quorum model, there is only one copy of the database stored on a special hardware disk and hence issues like data synchronization never occur.



A typical cluster implementation is shown in the following image:



**Figure 2.8** Sanctuary Database installation: Clustering

Every resource group is published in a virtual server, which is accessible to external clients via a unique IP address and name.

2. Install SQL Server, add this to the cluster to provide failback services, deploy SQL Server to all nodes and, finally, test your installation.



## Items Created During the Sanctuary Database Setup

During the Sanctuary Database installation, the following items are created:

**Table 2.1** Items created by the Sanctuary Database installation

Item	Purpose	Access
<i>Directory:</i> %INSTALLDIR%\DB	Contains all SQL scripts needed by Sanctuary's database setup	Full control for Administrators



**Note:** The %INSTALLDIR% directory points to the folder where the program was installed. It is usually C:\Program Files\Lumension Security\Sanctuary, but it can refer to any other folder.



## 3 Using the Key Pair Generator

To accompany the Sanctuary Management Console, Lumension provides the Key Pair Generator. This utility is used to create a key pair to assure the integrity of the communication between the Sanctuary Application Server and the Sanctuary Client. The information in this chapter is relevant to all Sanctuary products.

### Introduction

---

The Key Pair Generator is used to create a public and private key pair. The Sanctuary Application Server uses an asymmetric encryption system to communicate with the Sanctuary Client. The Sanctuary Application Server and kernel clients contain a default embedded key pair that is suitable for evaluation purposes only.



**Warning:** In a production environment, you must create your own key pair BEFORE installing the Sanctuary Application Server. This is done using the Key Pair Generation utility.

If you are using Sanctuary Device Control:



**Warning:** Never change the key pair after adding encrypted removable media in the Media Explorer. Doing so means that your users will no longer be able to recover a lost password of an encrypted media.



**Warning:** Never change the key pair during a Sanctuary upgrade when client hardening is switched on, otherwise your upgrade will fail.



**Note:** These keys are used to protect the communication between the Sanctuary Application Server and the client computers. They play also a role in the media encryption process but they are not media encryption keys.





**Note:** We recommend that you install and publish a Microsoft CA on your Active Directory structure before trying to encrypt a removable device.

## Starting the Key Pair Generator

1. Navigate to the `bin\tools\` directory found on your installation CD.
2. Run the `keygen.exe` tool.

The *Key Pair Generator* dialog is displayed.

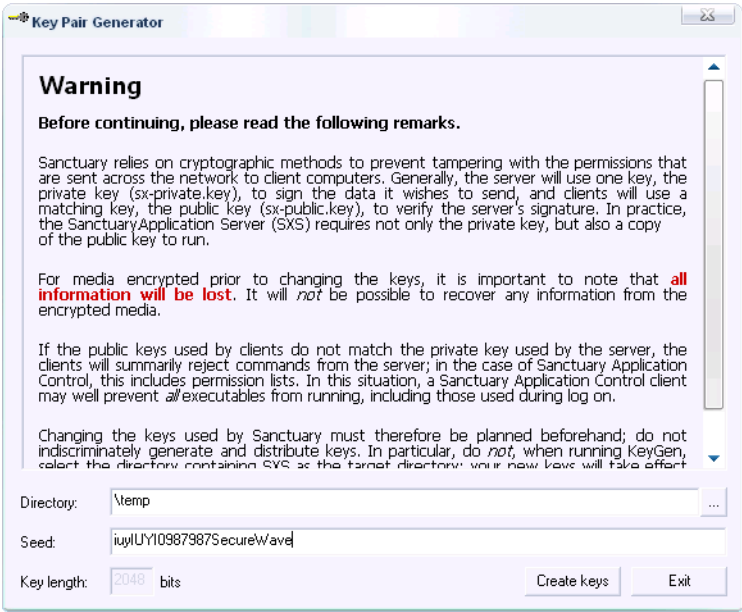


Figure 3.1 Key pair generation: First step

## Generating a Key Pair

1. Select the temporary directory in which you want to save the private and public key files.
2. Enter any random text into the *Seed* edit field. This is used to initiate the random number generator.



3. Click on *Generate*. The key pair is generated. A dialog similar to the following one is displayed:



**Figure 3.2** Key pair generation: Final message

4. Click on OK.

## Deploying the Key Pair

The key pair can now be distributed. To do this, copy the private key file 'sx-private.key' and the public key file 'sx-public.key' to the computer(s) where you will be installing the Sanctuary Application Server.

On startup the Sanctuary Application Server checks for the key pair in the following locations:

1. The directory where the Sanctuary Application Server executable is installed (usually %SYSTEMROOT%\SYSTEM32).
2. The Sanctuary Application Server's private directory, whose recommended location is %SYSTEMROOT%\SXSDATA.
3. All removable drives and DVDs/CDs in alphabetical order.

The search stops at the first valid key pair.



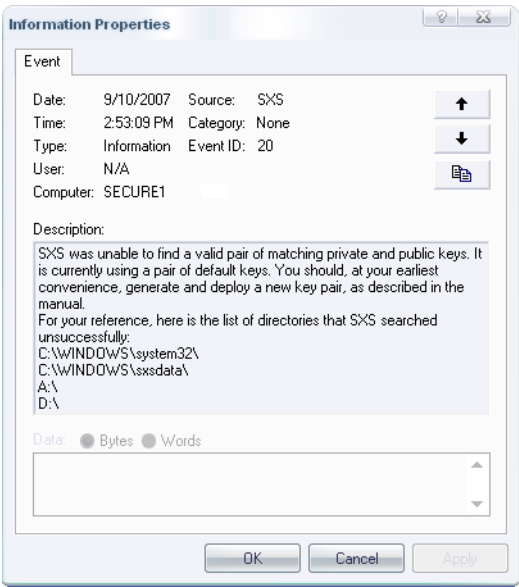
**Note:** When a new key pair is generated to replace an existing one, you must restart the Sanctuary Application Server service in order to start using the newly generated keys. The Sanctuary Application Server Service can be started and stopped through the Windows Services Panel or using a command line (`net stop sxs` and `net start sxs`).



**Note:** If the key pair is not in the %SYSTEMROOT%\SXSDATA directory, physical access to the servers running the Sanctuary Application Server should be strictly controlled because a rogue administrator could replace the key pair by inserting a removable media with a different key pair on it.



If Sanctuary Application Server starts and cannot find the key, it writes an event to the event log and uses the default key pair set provided by Lumension. This message does not correspond to a system malfunction; it indicates that all components work with default keys. This is not recommended for obvious security reasons.



**Figure 3.3** Sanctuary Application Server did not find the public-private key pair

ONLY the public key file `sx-public.key` should be deployed to all client computers by means of the Sanctuary Client setup. You should copy the Client folder from the product media to a network share and copy the `sx-public.key` into this folder. Setup will detect that a new public key is present and will copy it to the target computer.



**Note:** For machines that already have Sanctuary Client installed, copy the public key file (NOT the private key file) to the `%SYSTEMROOT%\SXDATA` directory of the client computer (typically `C:\WINDOWS\SXDATA`). You must reboot the machines to receive the new settings signed with the matching key pair.



## 4 Installing the Sanctuary Application Server

This chapter explains how to install the *Sanctuary Application Server* on the computers that are going to be servers for the application. Whereas [Chapter 1, “Installing Sanctuary’s Components”](#) provides an overview of the entire setup, this chapter focuses exclusively on the Sanctuary Application Server. The information in this chapter is relevant to all Sanctuary software suite products.



**Note:** Be sure to generate a key pair before proceeding to install the Sanctuary Application Server(s). See [Chapter 3, “Using the Key Pair Generator”](#) on page 29 for more information.

When you install the Sanctuary Application Server, a number of tools are copied to your hard disk. The installed tools are:

- The Sanctuary Application Server.
- The SXDomain Tool.



**Warning:** Although you can use Windows XP, 2000 Pro, or Vista x 86 for the database or/and console, you cannot use it for the Sanctuary Application Server (or client component in the case of Sanctuary Application Control Server Edition). If you are planning to spread Sanctuary components among several machines, one of them in an XP operating system — database and/or management console —, you should read carefully [Appendix D, “Installing Sanctuary Components on Windows XP/2003/Vista”](#) on page 175 before proceeding.

### Before you Install

Before you begin installing the Sanctuary Application Server, you must do the following:

- Make sure that the computer meets the minimum requirements (see on page for details).
- Have the database already installed on the computer that is to hold your information (see [Chapter 2, “Installing the Sanctuary Database”](#) on page 17 for details).
- Make sure that Microsoft Data Access Components (MDAC), version 2.6 SP1 or later, is installed.
- Generate the Key Pair (see [Chapter 3, “Using the Key Pair Generator”](#) on page 29 for details).





**Note:** If the server setup cannot find the MDAC component on your computer, it prompts you to download it from Microsoft web site. You must restart the setup after installing MDAC.

MDAC enables computers to connect to SQL Server databases. As MDAC is language-dependent, it is mandatory that you install the correct language version for your operating system.



**Note:** If you experience database connectivity problems when installing the Sanctuary Application Server, re-install MDAC on the computer hosting it.

- Ensure that the TCP/IP protocol is installed. This is required so that the Sanctuary Client running on the client computer can communicate with the Sanctuary Application Server. The setup program does not check this prerequisite.
- Ensure that the computer on which you want to install Sanctuary Application Server has a **fixed IP address**. This is recommended as the Sanctuary Client uses this address to connect to the Sanctuary Application Server. You need at least one valid IP address. DHCP (Dynamic Host Configuration Protocol) and server names can be used, provided that the DNS (Domain Name System) is set up correctly.



**Note:** We recommend using NAT (Network Address Translation) if you are running Sanctuary Application Server under VMWare.

- Ensure the Sanctuary Application Server can do a fully qualified domain name resolution of the clients it is going to manage. You have to set up the mechanism to translate clients' names into IP addresses.
- Create or use an existing account to be used by the Sanctuary Application Server service<sup>1</sup>. Setup automatically grant this account the rights to log on as a service<sup>2</sup>. You **MUST** use an account with local administration rights if you plan to use TLS protocol for Sanctuary Client - Sanctuary Application Server or intra-Sanctuary Application Server communications. See on page for more information.



**Note:** The service account must have the relevant permissions to read domain information, if any, from the Windows SAM (Security Account Management) database. One solution is to make the Sanctuary Application Server service account a member of the Domain Users group.

1. We will refer to this account as the Service Account
2. User right: Act as part of the operating system and impersonate a client after authentication.



**Note:** If you are installing the program on a computer that is a member of a workgroup (wired to other computers but not member of a domain) you may need to use an account with Administrative privileges to connect to the database. Using a non-privileged account requires that the Setup process adds Access Control Entries (ACEs) for the user and to several directories as well as granting the account the rights to connect and use the database.



**Note:** Setup verifies the specified password/account before proceeding. Setup continues if it fails to verify the password but will be interrupted, and rollback, if the password cannot be validated when creating the server service.

- Make sure that the Sanctuary Application Server service account has the right to access the database. If the database and Sanctuary Application Server are installed on the same computer, there will be no need to create such access, as it will be granted by our Setup. However, when the Sanctuary Database and Sanctuary Application Server run on two different computers, you must grant the service account the rights to connect and use the database. You can use the Microsoft SQL Server Enterprise Manager to grant domain users the right to log in and use the database (available with SQL Server only). If running SQL Server 2005 Express Edition, you will have to use the grantdb.exe command-line application for every service account you will use. This can be found in the \BIN\TOOLS folder of your Lumension CD.



**Note:** Sanctuary Application Server uses Windows Authentication mode to connect to the database. Start the 'Enterprise Manager' (or Management Studio) provided with your SQL Server, select your database server, expand this branch of the tree, and check the 'Security' node. This holds the Login definitions. By default, BUILTIN\Administrators have access. If the Sanctuary Database and the Sanctuary Application Server are on the same machine the account under which the Sanctuary Application Server runs is granted access to the database during setup. If the Sanctuary Database and the Sanctuary Application Server are on different machines, you must use grantdb.exe to allow the account to access the database.

- Get a license for your Sanctuary product. The license information is stored in a file called `Sanctuary.lic`. Your Sanctuary Application Server installation will fail without it. The file contains details of the licenses you have purchased, for example, the number of server and client copies. If you have purchased one of our Sanctuary products, this file is sent to you by email. If you are evaluating a Sanctuary product, then you can obtain an evaluation license by registering on the Lumension website ([www.Lumension.com](http://www.Lumension.com)), selecting the appropriate product page, and completing an Evaluation License Request form. Once you have a copy of the license file, save it into the %SYSTEMROOT%\SYSTEM32 directory. If your license has expired, Sanctuary Application Server services do not start and a warning message is displayed.





**Warning:** If you are using more than one Sanctuary Application Server the same license file must be used on all the servers. **Never** place this license file in any client.

- (Optional). Check that the computer(s) running Sanctuary Application Server also has a system clock synchronization mechanism to match that of the computer running the database. You can use Windows Time Service (W32Time, based on Simple Network Time Protocol or SNTP) to maintain date and time synchronization.
- Have a Certificate Authority installed and ready to provide your Sanctuary Application Server machine with a valid certificate if you are planning to use TLS (Transport Layer Security) protocol to communicate between Sanctuary Application Servers (if you are planning to install more than one) and/or Sanctuary Application Server-client communications. See [“Transport Layer Security”](#) on page 6 and [Appendix H, “Installing a Certificate Authority for Encryption and TLS Communication”](#) for more information.



**Warning:** The decision to use or not TLS should not be taken lightly. Once you decide to use TLS for your client-Sanctuary Application Server and/or intra-Sanctuary Application Server communications and install Sanctuary in this mode, it is very difficult to roll this back and you will need to completely uninstall all Sanctuary’s components and modify registry keys.

## To Install the Sanctuary Application Control

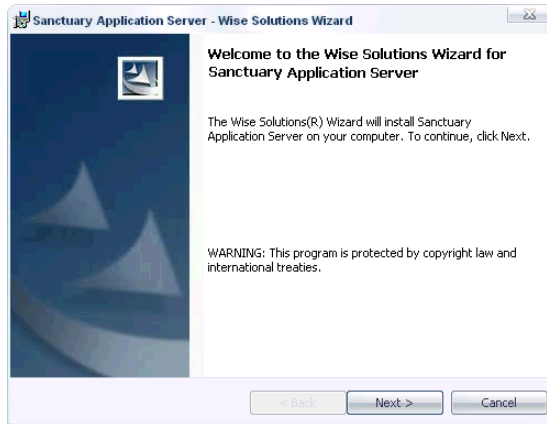
---

The Sanctuary Application Server handles client logons and is the only component that connects to the database.

1. Log on to the computer that is going to hold the Sanctuary Application Server component. The account you use must have:
  - Administrative rights.
  - Access to SQL Server.
2. Close all programs running on the computer.
3. Insert the Sanctuary CD in your DVD/CD drive and run setup.exe located in the \SERVER\sxs folder.



The *Welcome* dialog is displayed.



**Figure 4.1** Sanctuary Application Server installation: First step

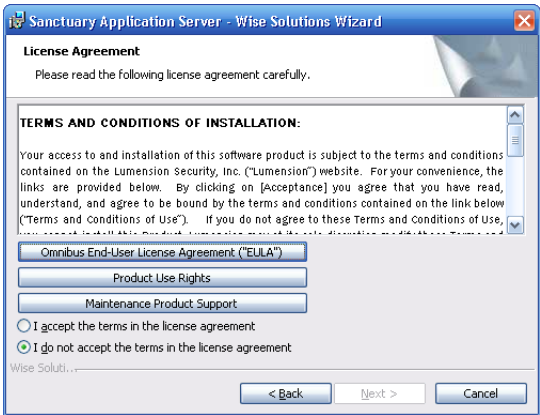
4. Click on the NEXT button to continue.



**Warning:** The Setup does not generate a log file if it is launched running the sanctuaryserver.msi file instead of the setup.exe file. The log file may be important in case of troubleshooting and when contacting Lumension.

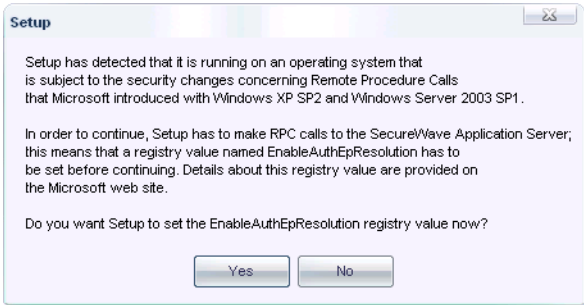


The next dialog displays the *License Agreement*.



**Figure 4.2** Sanctuary Application Server installation: License agreement

- 5. If you accept the terms of the license agreement, select the **“I accept the terms in the license agreement”** option and click on **Next**. You can also click on any of the three available buttons to read the license agreements.
- 6. If you are using an operating system subject to security changes concerning the RPC (Remote Procedure Call) protocol (Windows XP SP2 or Windows Server 2003 SP1 or SP2), the registry key ‘EnableAuthEpResolution’ must be changed:

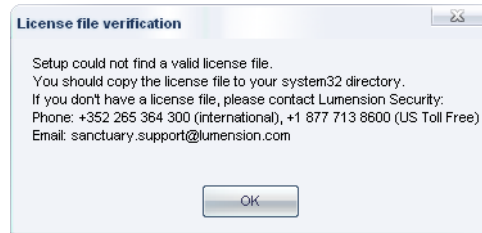


**Figure 4.3** Sanctuary Application Server installation: RPC warning

See [Appendix D, “Installing Sanctuary Components on Windows XP/2003/Vista”](#) for more information.



The installation program checks for the presence of a valid license file. If the setup program cannot find one or the file was altered in any way (e.g. due to an email filter introducing linefeed characters or translating foreign characters), an error message is displayed.



**Figure 4.4** Sanctuary Application Server installation: No license found

7. If you have a license file and see an error message, check the name of the `Sanctuary.lic` file and copy it to the `%SYSTEMROOT%\SYSTEM32` folder.

If this does not resolve the problem, check your email client settings, verify that your license file does not have a `.txt` extension which may be hidden in Windows Explorer, or contact Lumension's technical support team to obtain a new license file.



**Note:** The setup will refuse to install Sanctuary Application Server if it cannot find a valid license.

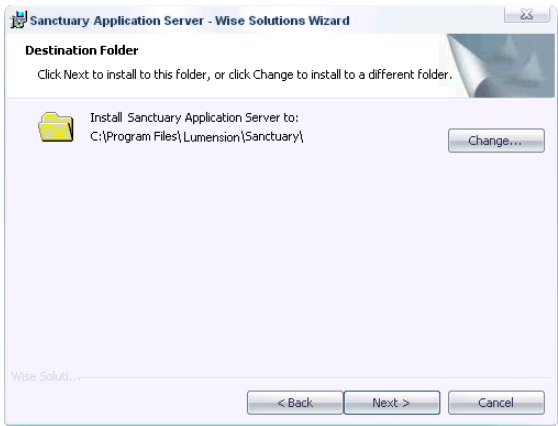


**Warning:** If you are using more than one Sanctuary Application Server the same license file must be used on all your servers.

8. Choose the folder in which you want to install the Sanctuary Application Server and click on NEXT. By default, the database is installed in the `C:\Program Files\Lumension Security\Sanctuary` folder. To choose another location, click on CHANGE and browse to the folder you want. Some components are always installed on the

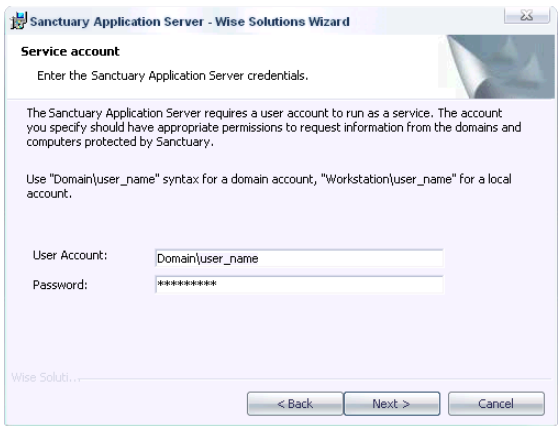


%SystemRoot%\system32 directory and a %SystemRoot%\sxldata directory is always created.



**Figure 4.5** Sanctuary Application Server installation: Destination folder

- 9. Specify the user account you want to use to run the Sanctuary Application Server. Use a domain account (any domain user, an administrative account is not required) if you plan to use Sanctuary in a domain environment. Use a local account if you plan to manage several computers in a workgroup or a Novell environment.



**Figure 4.6** Sanctuary Application Server installation: Service account





Domain accounts should be entered as DOMAIN\User while local accounts should be prefixed by the computer name (e.g. COMPUTER\User).

The domain specified here will be the one that gets synchronized, by default, at the end of the setup.

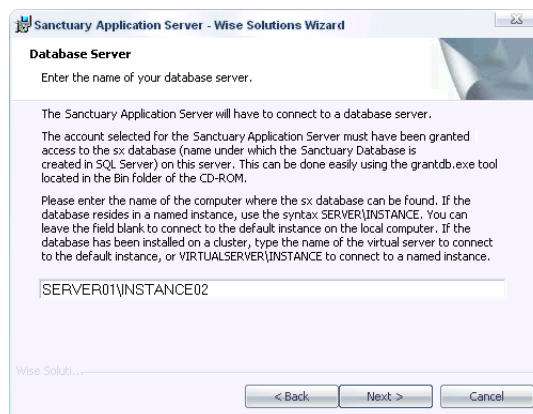


**Note:** Setup checks the validity of the password. You must precede the user name with the domain or workstation name and a backslash (\). The account you enter must have full access to the database and the computer containing the DataFileDirectory where the Sanctuary Application Server log, shadow and history files are stored.



**Warning:** Before attempting to connect to a remote server, you must grant the service account the rights to connect and use the database. You must, therefore, log on to the computer where the SQL Server or Client is running and grant the user the necessary rights either by means of the SQL Server Enterprise Manager or using the grantdb.exe utility located in the \BIN\TOOLS folder of the Lumension CD. Local users should be mirrored (same user name and password on both servers).

10. Specify the SQL Server instance that Sanctuary Application Server should connect to. To do this, enter the name of the machine, or the virtual server name in case of a cluster server. If the database does not reside on a default instance, you should suffix the server name with a backslash and the SQL Server instance name where you installed the Sanctuary Database (sx).



**Figure 4.7** Sanctuary Application Server installation: Sanctuary Database server location

11. Click on NEXT to continue.

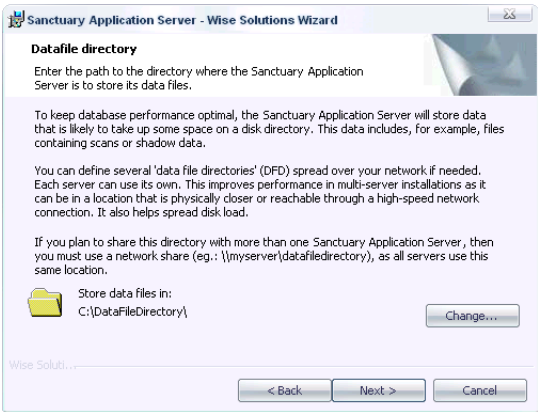


The syntax used to enter the name of your database server depends on where you installed the *Sanctuary Database*. Here is a summary of the different cases:

**Table 4.1** Database server name syntax

Sanctuary Database server	The Sanctuary Database is created in the default instance	The Sanctuary Database is created in a Named instance
The database is on the local computer.	ServerName or leave the field blank	ServerName\InstanceName
The database is on another server.	ServerName	ServerName\InstanceName
The database is on a cluster (local or remote).	VirtualServerName	VirtualServerName\InstanceName

12. Choose the folder where you want the Sanctuary Application Server log, shadow, or/and scan files are to be stored. Setup will suggest a directory named DataFileDirectory (DFD) under the system’s drive root. You should use a permanent network share if you are planning to install more than one Sanctuary Application Server or a dedicated file server. All servers can optionally write to the same, shared, directory or you can opt for having different ones for each server (see [Figure 1.1](#)). For evaluation purposes, use a single DFD in a local directory.



**Figure 4.8** Sanctuary Application Server installation: Data file directory



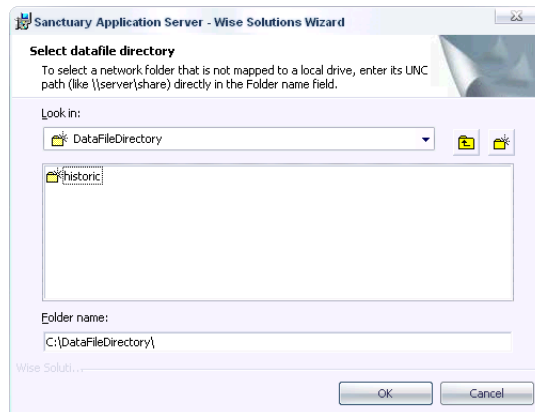


**Note:** You can have several ‘data file directories’ (DFD, see [Figure 1.1](#)) defined and spread over your network to be used by the Sanctuary Application Server(s). Each server can use its own. This improves performance in multi-server installations as each server can be configured to store its data files in a location that is physically closer, or reachable through a high-speed network connection. It also helps spread disk load, as each defined directory only contains part of the files. Note that it is still possible for more than one server to use the same DFD, all servers can still access all data files — it does not matter if only one or multiple directories are used, when a server does not find a file in its defined directory, it requests a copy from a server having access to it.



**Warning:** You should pay special attention to the network share security (ACL) and Directory NTFS permissions. Limit access to the server service account and optionally to some administrators. You will also need to consider the members of the ‘Power Users’ group.

13. If you want to change the directory location or if you are installing more than one Sanctuary Application Server, select a shared network folder. To do this, click on CHANGE and locate the path you want to use for the DataFileDirectory:



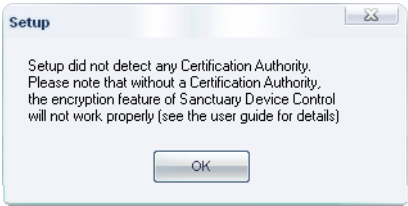
**Figure 4.9** Sanctuary Application Server installation: Change destination folder



**Note:** Always use a Universal/Uniform Naming Convention (UNC) path name, for example, \\server\volume\directory. Do NOT use a mapped drive.

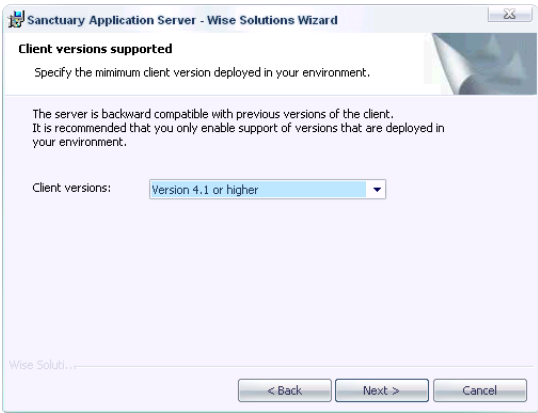


If you are installing Sanctuary Device Control and do not have a Certification Authority installed, the following warning message is displayed:



**Figure 4.10** Sanctuary Application Server installation: No Certification Authority found

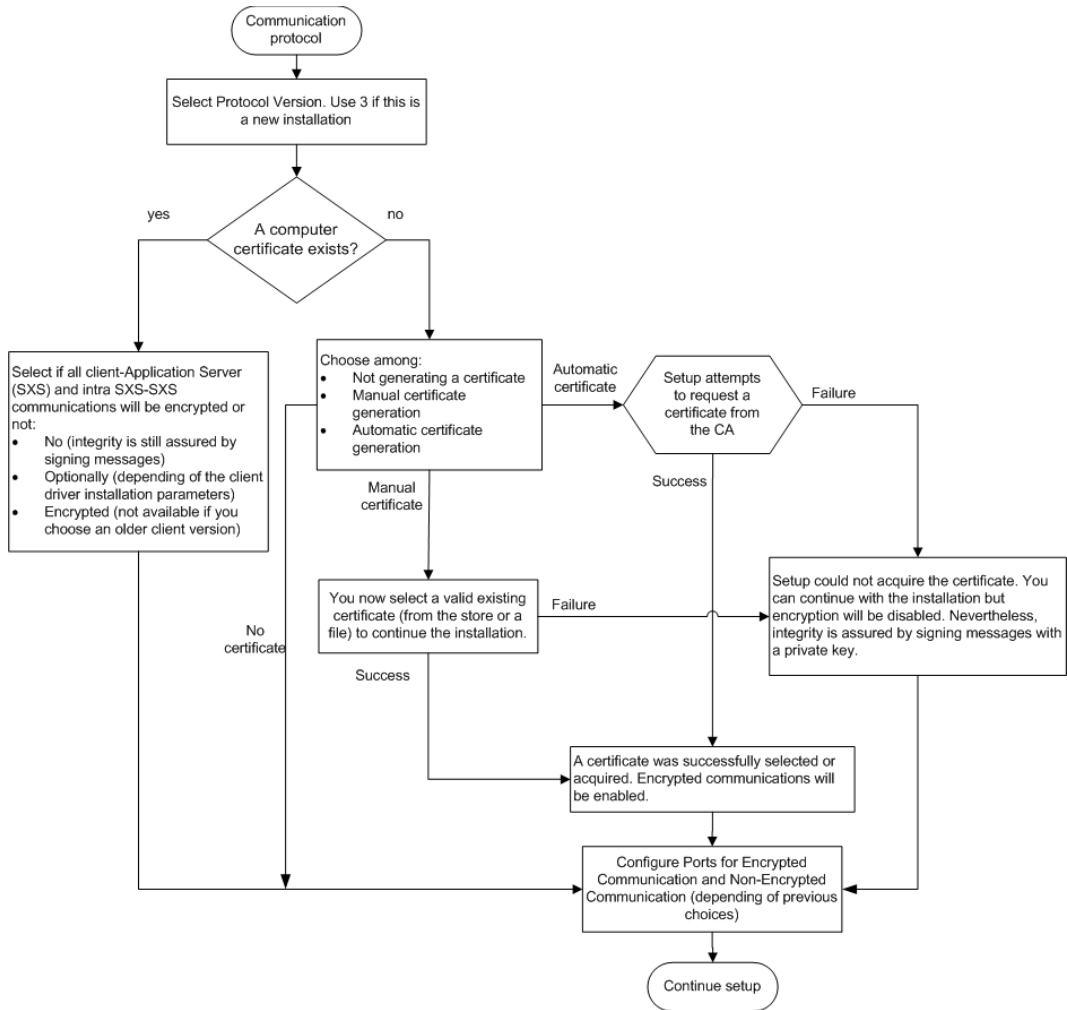
- 14. Specify the protocol that Sanctuary Application Server should use. You can either choose the standard one, used to communicate with older clients, or the improved protocol, which includes optional TLS protocol that only works with the latest client version. Select from the list the type of client you already have installed. If this is a new installation, select the latest version.



**Figure 4.11** Sanctuary Application Server installation: Protocol selection dialog



15. For the rest of the installation, follow the flowchart below (especially if you choose the latest version of the client):



**Figure 4.12** Sanctuary Application Server installation: Protocol selection flowchart



The following screens may appear, depending of the options selected (as stated in the flowchart depicted in [Figure 4.12](#)):



**Figure 4.13** Sanctuary Application Server installation: No certificate



**Figure 4.14** Sanctuary Application Server installation: Valid certificate, old clients



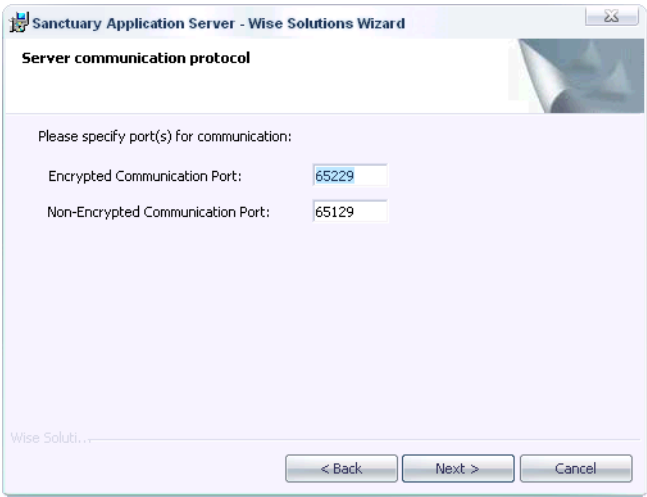


**Figure 4.15** Sanctuary Application Server installation: Valid certificate new clients



**Figure 4.16** Sanctuary Application Server installation: Could not retrieve or generate a valid certificate





**Figure 4.17** Sanctuary Application Server installation: Communication port configuration



**Note:** You should only configure the ‘Communication Port’ fields when the proposed ones are used by another software application or blocked for security reasons.



**Note:** The parameters selected in the previous dialogs should also be used if you are installing more than one Sanctuary Application Server. See [“Using TLS for the Inter-Sanctuary Application Server Communication”](#) on page 10 for more information.



**Note:** For a detailed manual tuning, see [Table B.6](#) on page 160 and [Table B.7](#) on page 161.

When the *Automatic request certificate* option is selected, the program attempts to obtain a valid certificate by requesting it to the Certificate Authority. If this fails, the installation can continue but communication’s encryption is deactivated. Nevertheless, integrity is assured by signing the messages with a private key (see [Chapter 3, “Using the Key Pair Generator”](#)).



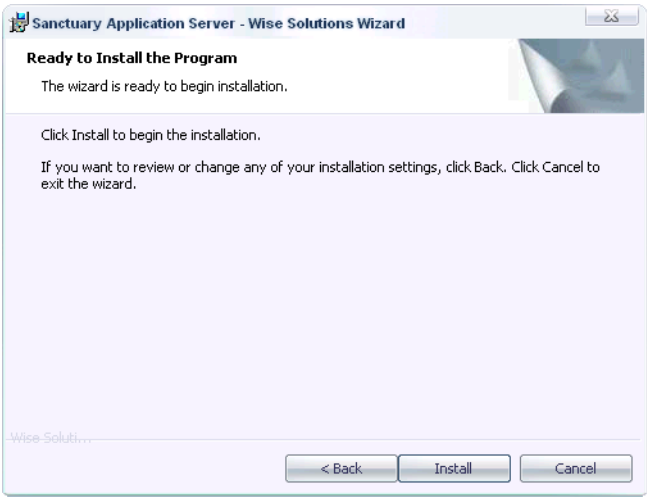
If you select the manual option, a new dialog opens where you are invited to select the location where a valid machine certificate can be found — you must already have a Certificate Authority installed or the required certificate at hand. See [Appendix H, “Installing a Certificate Authority for Encryption and TLS Communication”](#) for more details. The available options are the same ones described for the client installation (found in “[To Install Sanctuary Clients](#)” on page 63).



**Figure 4.18** Sanctuary Application Server installation: Server authentication certificate location



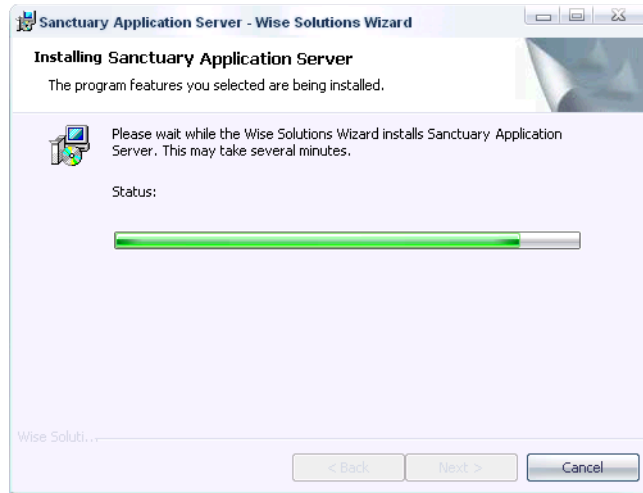
Setup is now ready to install the Sanctuary Application Server Component.



**Figure 4.19** Sanctuary Application Server installation: Final stage

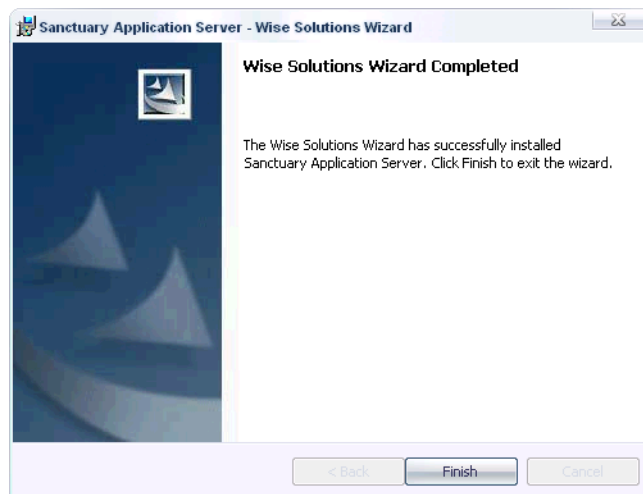
- 16. Click on **INSTALL** to proceed. A warning message is displayed if you are not using a fixed IP address.

Setup gathers information about the domain structure. It retrieves the names of the domain users, groups, and machines from the domain controller. This may take several minutes (up to half an hour), depending on the size of the domain and connection speed.



**Figure 4.20** Sanctuary Application Server installation: Installation

The final dialog indicates when the installation has been successfully completed.



**Figure 4.21** Sanctuary Application Server installation: Finishing the installation



17. Click on FINISH to close the wizard.
- You now have a working Sanctuary Application Server connected to the *Sanctuary Database*.

Items Created During Sanctuary Application Server Setup

During the Sanctuary Application Server installation, the setup creates the following items:

Table 4.2 Items created by the Sanctuary Application Server installation

Item	Purpose	Access
Directory: C:\DataFileDirectory	Directory where the Sanctuary Application Server logs, and shadow files are stored.	Full control for Administrators
Directory: %INSTALLDIR%\SXTools	Folder where the FileTool, KeyGen, and SXDomain auxiliary tools are placed. You can find a full description of these tools in the corresponding administrator's guide and in this setup guide.	Full control for Administrators, Read/Execute for authenticated users.
Directory: %INSTALLDIR%\SSF	Contains all Sanctuary Application Server support files and tools.	Full control for Administrators, Read/Execute for authenticated users.
Registry keys*: HKLM\system\CurrentControlSet\services\sxs\parameters	See <a href="#">Appendix B, "Registry Keys"</a> for a complete description.	n/a
*You can block the use of the RegEdit.exe program for all users by using our Sanctuary Application Control Suite		



**Note:** The %INSTALLDIR% directory points to the folder where the program was installed. It is usually C:\Program Files\Lumension Security\Sanctuary, but can refer to another folder.

## 5 Installing the Sanctuary Management Console

This chapter explains how to install the *Sanctuary Management Console* used to configure permissions to all the devices and/or executables that your organization uses. It is also used to carry out day-to-day administrative tasks and procedures. The information in this chapter is relevant to all Sanctuary software suite products.



**Warning:** You should read [Appendix D, “Installing Sanctuary Components on Windows XP/2003/Vista”](#) on page 175 carefully before installing this component on a computer with this operating system and service pack.

When installing the Sanctuary Management Console you also install some or all of the following, depending on the type of license you have purchased:

- The *Client Deployment Tool* (see [Chapter 8, “Unattended Client Installation”](#) on page 93) to deploy clients silently.
- The *Svolbro.exe* program (see description in the *Sanctuary Device Control User Guide*) needed for one of our USB key encryption methods.
- The *Authorization Wizard* (see description in the *Sanctuary Application Control Suite User Guide*) to search for executable files, create their hashes, and include them in the database.
- The *Versatile File Processor Tool* (see description in the *Sanctuary Device Control User Guide*) to scan files.
- The *Standard File Definitions (SFD)*: set of all the hashes (digital signatures) of various operating systems files supported by Sanctuary.



**Note:** If you are using Sanctuary Application Control Suite, you should also consider installing the Authorization Service (see the *Sanctuary Application Control Suite User Guide*) to monitor changes and create updates (using Microsoft’s SUS or WSUS).

### Before you Install

Before you begin the installation of the Sanctuary Management Console, you must:

- Ensure that the computer(s) meet the minimum requirements. See [Appendix A, “Detailed System Requirements and Limitations”](#) on page 147 for details.
- Ensure that the *Sanctuary Database* and *Sanctuary Application Server* have been installed, either on this computer or on other computers within your network. Refer to the previous chapters.

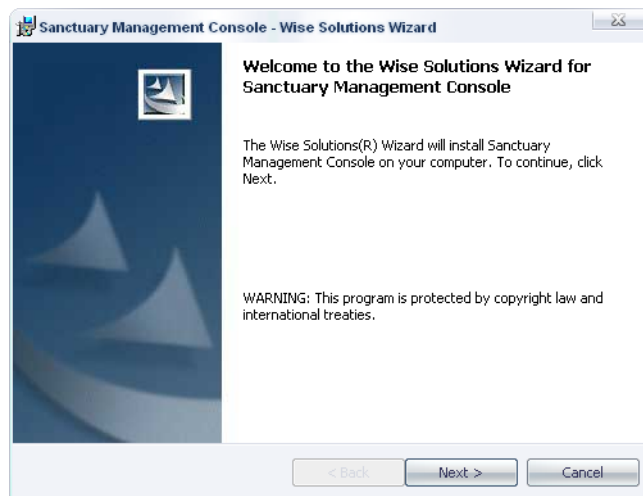


### To Install the Sanctuary Management Console

---

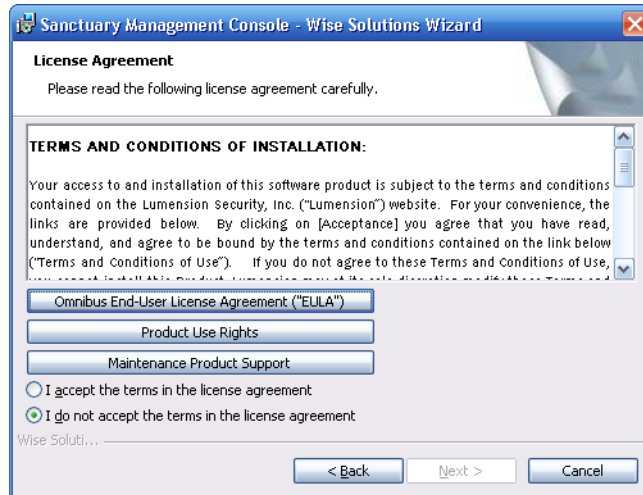
To install the *Sanctuary Management Console*, follow these steps:

1. Log on with an account that has administrative privileges in the computer in which you are installing the Sanctuary Management Console.
2. Close all programs running on the computer.
3. Insert the Sanctuary CD in your DVD/CD drive and run setup.exe located in the \Server\smc folder.



**Figure 5.1** Sanctuary Management Console installation: First step

The next dialog displays the *License Agreement*.



**Figure 5.2** Sanctuary Management Console installation: License agreement

4. If you accept the terms of the license agreement, select the **“I accept the terms in the license agreement”** option and click on **Next**. You can also click on any of the three available buttons to read the license agreements.



**Note:** The license agreement text is installed with the program. If you want to review it later, select ‘License agreement’ from the Start → Programs → Sanctuary menu..



- 5. Choose the destination directory, and other features — making a complete or custom installation.

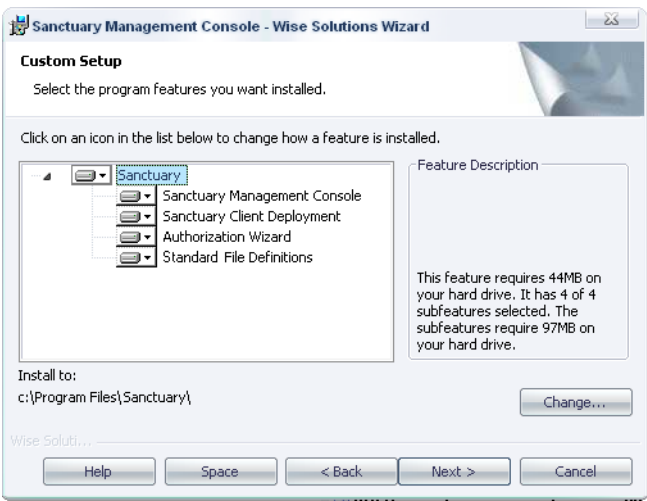


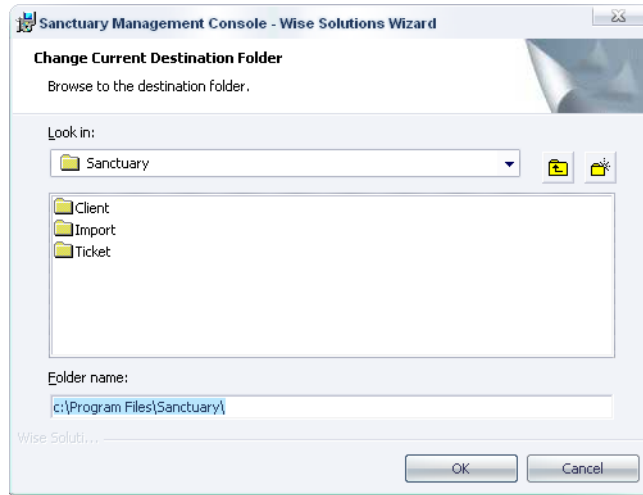
Figure 5.3 Sanctuary Management Console installation: Custom setup



**Note:** The Sanctuary Management Console allows you to configure, manage, and monitor permissions to devices/executables. You use the Client Deployment tool to deploy silently clients on a group of computers. The Authorization Wizard allows administrators to quickly identify and authorize executables. File Definitions let you rapidly populate your database with signatures of all the files needed for running your operating systems.



6. If you decide to modify the default installation location, click on **CHANGE** and select a local path to install the components and documentation. By default, the files are copied to the %ProgramFiles%\Lumension\Sanctuary\Console directory.

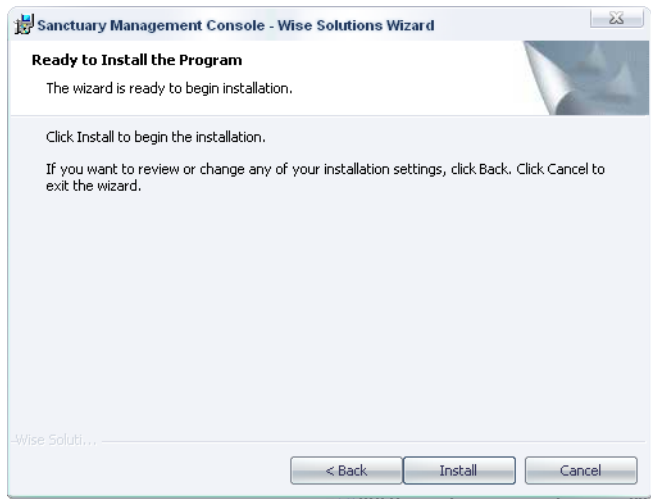


**Figure 5.4** Sanctuary Management Console installation: Modify destination folder

7. Click on **OK** to continue the installation.

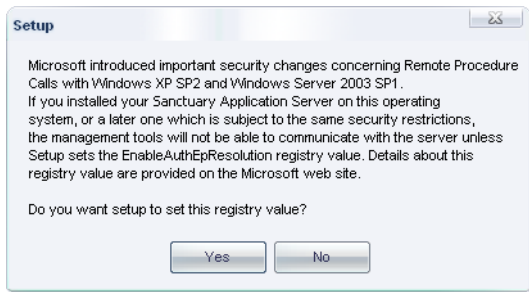


Now Setup is ready to install the files.



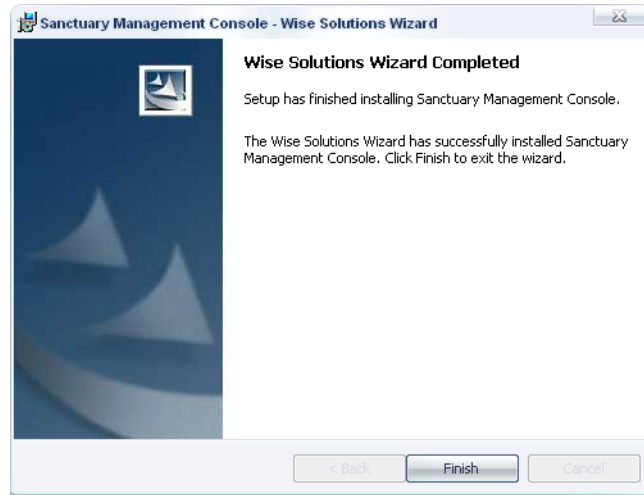
**Figure 5.5** Sanctuary Management Console installation: Ready to install

- 8. Click on **INSTALL** to start the installation process. This takes approximately 2 minutes, depending on the components selected and the hardware used.
- 9. If the computer is running Windows XP SP2 or Windows 2003 SP1 (or later), click on **YES** to continue. In this case, Setup needs to adapt the Windows settings to allow RPC communication between the Sanctuary Management Console and the Sanctuary Application Server. See [Appendix D, “Installing Sanctuary Components on Windows XP/2003/Vista”](#) on page 175.



**Figure 5.6** Sanctuary Management Console installation: Remote Procedure Calls warning

The final dialog indicates that the installation has been completed successfully:



**Figure 5.7** Sanctuary Management Console installation: Finishing the installation

10. Click on the FINISH button to close the dialog and end the procedure.

By default, only users that are members of the Administrators group of the computer running the Sanctuary Application Server can connect via the Sanctuary Management Console. You should define who can manage and define policies by selecting *User Access* from the *Tools* menu of the Sanctuary Management Console. See the relevant *Administrator's Guide* for further information.



**Note:** If you are installing Sanctuary Device Control, we strongly recommend that you also install the Sanctuary Client on all computers having the Sanctuary Management Console. If you do not install it on the administrator's computer, it is not possible to use media encryption or to authorize multi-sessions DVDs/CDs with the Media Authorizer. See [Chapter 6, "Installing the Sanctuary Client on Your Endpoint Computers"](#) on page 61 for more details.



## Items Created During Sanctuary Management Console Setup

During the Sanctuary Management Console installation, the setup creates the following items:

**Table 5.1** Items created by the Sanctuary Management Console installation

Item	Purpose	Access
Directory: %INSTALLDIR%\Console	Contains all Sanctuary Management Console EXE and DLL files.	Full control for Administrators, Read/Execute for authenticated users.
Directory: %SYSTEMROOT%\Help	Sanctuary Management Console help files.	Full control for Administrators, Read/Execute for authenticated users
Shortcuts	All Windows' Start→Programs menu shortcuts	n/a
*You can block the use of the RegEdit.exe program for all users by using our Sanctuary Application Control Suite component.		



**Note:** The %INSTALLDIR% directory points to the folder where the program was installed. It is usually C:\Program Files\Lumension Security\Sanctuary, but can refer to another folder. %SYSTEMROOT% is usually C:\Windows.



## 6 Installing the Sanctuary Client on Your Endpoint Computers

The Sanctuary Client is the software used to manage the devices and/or applications on the endpoint computer/servers. This chapter explains how to install the client on the endpoints you want to manage when you only have a few computers in your system, or for testing purposes. To deploy our client in large organizations, or when you cannot visit each computer individually, we recommend using our specialized software tool, described in [Chapter 8, “Unattended Client Installation”](#).

The Sanctuary Client communicates with the Sanctuary Application Server(s) to retrieve application/device control policies. This is done using a TCP/IP connection with a signed (always) or encrypted communication — depending on the installation options. If this connection cannot be established using the Fully Qualified Domain Names (FQDN) or IP addresses, the driver tries to use the Proxy configured for Internet Explorer — if available – to locate a valid Sanctuary Application Server. See any of the administrator’s guide architecture section for more info on how to configure this proxy connection.



**Warning:** Please read [Appendix D, “Installing Sanctuary Components on Windows XP/2003/Vista”](#) on page 175 carefully before installing this component on computers that use this operating system and service pack. Although you can use Windows XP for the database and console, you cannot install the Sanctuary Application Control Server Edition client on it. We do not support Windows XP, 2000 Pro, or Vista for Sanctuary Application Control Server Edition (client component).



**Warning:** Please disable Windows’ System Restore (Windows XP or Vista) feature before installing the client. If you try to roll back to a previous state after installing the Sanctuary Client, the system becomes unstable. This is a System Restore design limitation since it will not reinstate all files completely. Be aware that System Restore is not a substitute for uninstalling a program. Since this is a specific Windows feature, you must search your Window’s help file to find out how to disable your System Restore points before proceeding (using the Control Panel or Policies).

### System Requirements

The system requirements can be divided into what is needed for the overall system and what is needed for each client computer.

#### Overall System Requirements

Before you install the Sanctuary Client on a client computer, you must:



- Ensure that the *Sanctuary Database*, *Sanctuary Application Server*, and *Sanctuary Management Console* are already installed on their respective computers.
- Make sure that the domain information stored in the database is up to date. If necessary, update it using the *Tools* → *Synchronize Domain Members* menu in the *Sanctuary Management Console*.
- Define the appropriate, or at least minimum, policies that are to be used by the clients. Failing to do so *WILL* result in users being denied access to their executable files (event the operating system, blocking the user from his machine) and/or devices connected to their computers. If you are using Sanctuary Application Control Server Edition or Sanctuary Application Control, confirm that the *Blocking Mode* option is set to *Non Blocking Mode*, in the *Default Options* dialog of the console.
- If you have already installed the client using the Client Hardening mode, and want to uninstall/ modify/ repair it, issue an 'Endpoint Maintenance Ticket', using the management console, and copy it to the required directory. Please consult your corresponding *User's Guide* and "[Sanctuary Client Registry Keys](#)" on page 163 for more information. If you are using our client deployment tool, you only need to specify a valid Sanctuary Application Server address from where the ticket is obtained.
- If you are planning to use the TLS protocol for your client, have a valid certificate issued by your Certificate Authority installed and configured (as explained in the [Appendix H, "Installing a Certificate Authority for Encryption and TLS Communication"](#)).



**Warning:** The decision whether or not to use encrypted communications (TLS protocol) should not be taken lightly. Once you decide to use TLS for your Sanctuary Client - Sanctuary Application Server and/or intra-Sanctuary Application Server communications and install Sanctuary in this mode, it is very difficult to roll this back: You must completely uninstall all Sanctuary's components and modify registry keys.

### Client Computer Requirements

Make sure that the computer meets the minimum hardware and software requirements. See [Appendix A, "Detailed System Requirements and Limitations"](#) on page 147 for details.



**Warning:** If the target computers have been installed using prepared hard-drive images (for example using Symantec Ghost, Powerquest Driveimage, etc.) please make sure that every machine has received a different SID (Security Identifiers) and a different name before starting the deployment. You can use GhostWalker.exe, SidChanger.exe, etc., to do this.



**Note:** Although the installation dialog only lets you input three Sanctuary Application Servers, you can easily add more if needed. You can also change how the Sanctuary Application Server(s) is selected — round robin vs. random pick. All this is done by modifying certain registry keys. See [“Sanctuary Client Registry Keys”](#) on page 163 and [“Uninstalling the Sanctuary Client”](#) on page 79 for more details. You can ‘push’ these modifications to all clients using Group Policies with ADM templates.



**Note:** The setup also lets you retrieve a ‘Maintenance ticket’ from the Sanctuary Application Server (see the relevant Administrator’s Guide). This is only done if a communication between them exists. If the ‘client hardening’ is enabled — the uninstall process allows you to choose how to deactivate it.

## To Install Sanctuary Clients

---

The first step in this procedure is to decide whether or not you want to import the company’s permissions and policies as an independent file during the installation process. If you want to import them during the client installation, you first need to export them. This export is done to a special file called *policies.dat* that should be located in the same directory as the MSI installation file package. The files needed to install the client are located in the client folder of your installation CD. You can copy them to a convenient location on your hard disk. You should also include the public key — not the private one — in this directory. Proceed with the installation steps as described below carefully reading step 7: Providing the Sanctuary Application Server address.



**Note:** The policies.dat file should be accessible to the installation program. Be aware that if you place it in a network share — only valid for Active Directory environments — the computer account must have access to it.

See the *To export and import permission settings* section of the relevant *User’s Guide* for more information about how to export your settings to a file.

The *policies.dat* ‘import file’ is particularly useful when doing client installations on machines that are not actually connected to the network or that cannot communicate with the Sanctuary Application Server.



**Note:** The policies.dat file has a validity period of 14 days (default value) after which the setup refuses to use it.



In the next step you must specify whether or not you are using TLS protocol for Sanctuary Client - Sanctuary Application Server communications. If using TLS, all transmissions are fully encrypted. If the TLS is not selected, all communications are signed using the key pair previously generated. See [Chapter 3, “Using the Key Pair Generator”](#) on page 29 for more information about how to create these keys.

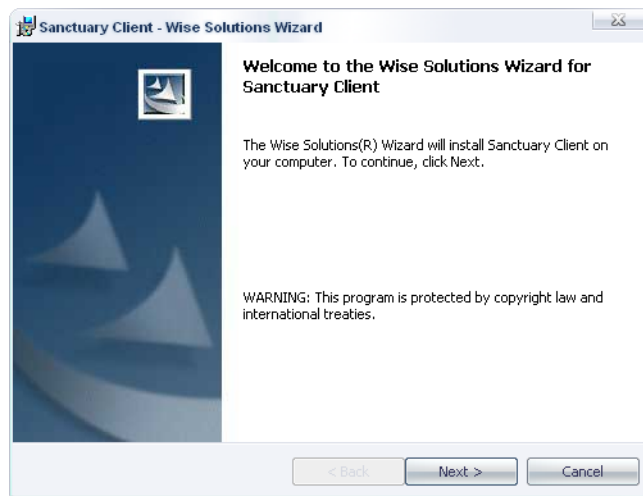
To install the Sanctuary Client on your client computers, follow these steps on each client computer:

1. Log on to the client computer using an account that has administrative rights.
2. Close all programs running on the computer.
3. Select the Client folder on the Sanctuary CD or navigate to the network shared drive where the Sanctuary Client setup files are located, and run the setup.exe file.



**Warning:** If you are installing or uninstalling the Sanctuary Client on a Vista machine with Vista's UAC (User Account Control) functionality turned on, you must use setup.exe (not using Control Panel → Add/Remove Programs) otherwise the operation will fail.

The Setup program shows the *Welcome* dialog:



**Figure 6.1** Sanctuary Client: First step

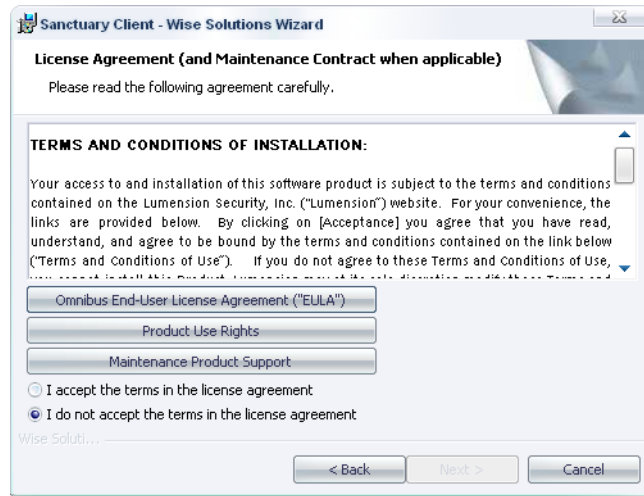
4. Click on NEXT to continue.





**Warning:** You cannot carry out maintenance (if the Client Hardening option is active) if you do not first issue an ‘Endpoint maintenance ticket’ or relax the client security settings using the management console. See “[Uninstalling the Sanctuary Client](#)” on page 79 for more information.

The next dialog displays the *License Agreement*.



**Figure 6.2** Sanctuary Client: License agreement

5. If you accept the terms of the license agreement, select the “**I accept the terms in the license agreement**” option and click on **Next**. You can also click on any of the three available buttons to read the license agreements.



6. Specify whether or not you want the Sanctuary Client to use the TLS protocol to communicate with Sanctuary Application Server (see [“Transport Layer Security”](#) on page 6).



**Figure 6.3** Sanctuary Client: Communication protocol

You can install the Sanctuary Client installation in one of three modes:

- ‘Server is using unencrypted protocol’ — No TLS. All communication between Sanctuary Client and Sanctuary Application Server(s) is not encrypted but is signed using the private key. This is, essentially, a legacy communication protocol and not recommended for high security installations.
- ‘Authentication certificate will be generated by setup’ — Manual mode using TLS communication.

The administrator generates and provides the machine certificate that is used in all communications. All communication between Sanctuary Client and Sanctuary Application Server(s) is encrypted. This mode is used when there is no Certification Authority installed in the network or the CA cannot be reached when doing the client installation. The machine certificate has to be created by a user (usually the administrator) who already possesses a certificate that can be issued and who trusted as a root or intermediate Certificate Authority by the Sanctuary Application Server. This authorized user has to be physically present at the machine to create the required certificate.

- ‘Authentication certificate will be retrieved from a CA’ — Automatic mode using TLS communication.

The program attempts to obtain a valid computer’s certificate by requesting one from one of the selected Certificate Authorities. This certificate must be able to be issued and the CA trusted as a root or intermediate Certificate Authority by the Sanctuary Application Server. All communication between Sanctuary Client and Sanctuary Application Server(s) is encrypted. You do not need a Certificate Authority at this point, but it is required when you first start the client(s), since the program requests a machine certificate. The user who has the rights to create machine’s certificates does not have to be physically present at the machine to do the installation if this mode is selected.

You should ALWAYS use automatic mode when your organization has already deployed a Certificate Authority infrastructure and the Sanctuary Application Server and clients are part of it. In this case, deployment of Sanctuary Client using TLS is completely transparent and requires no additional action.

We recommend you use the automatic mode in preference to all other methods for issuing valid certificates. If it is not possible to use this mode, then you should use the semi-automatic mode if you are using our Client Deployment Tool (see [Chapter 8, “Unattended Client Installation”](#) on page 93), and manual mode in all other cases.

Although you can select the port default values, you can always change them, if desired, to fine-tune the communication protocol by modifying the corresponding registry entries. See [Appendix B, “Registry Keys”](#) for more information.

Remember that you require a valid certificate on both machines (the one with Sanctuary Application Server and the one with the Sanctuary Client) in order to use a TLS channel that encrypts all communication. Even if you are not using TLS, all data transfer is signed with the private key generated before installing the Sanctuary Application Server. See [Chapter 3, “Using the Key Pair Generator”](#) on page 29 for more information about how to create these keys.



If selecting the second option, you should already have a valid machine certificate (i.e. not one that is revoked or has expired). The following screen is displayed, as:



Figure 6.4 Sanctuary Client: Communication protocol

TLS protocol uses a certificate to encrypt messages sent over the channel. In this dialog, you can select the machine’s certificate location and its parameters. When selecting the computer certificate’s parameters you can choose the service provider, key length, validity, and signature shown below:

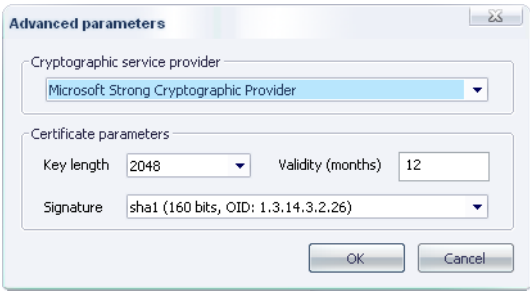
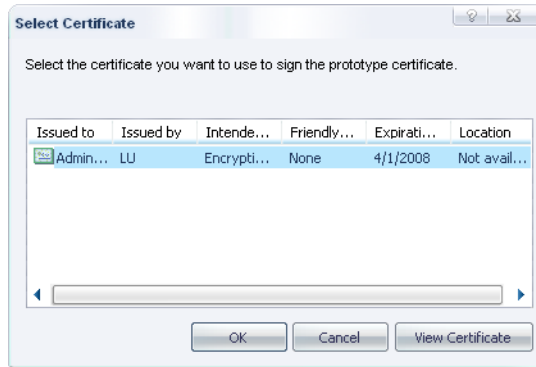


Figure 6.5 Sanctuary Client: Certificate’s parameters



If you select Import into store, Windows' Certification Wizard opens to allow you to retrieve the computer certificate. All other options require a valid certificate to exist in a store (special location where the Certificate authority saves valid certificates) or directly in a file that is imported to the local certificate store. An administrator can generate a valid one using the MMC console (Start→Run→mmc.exe):

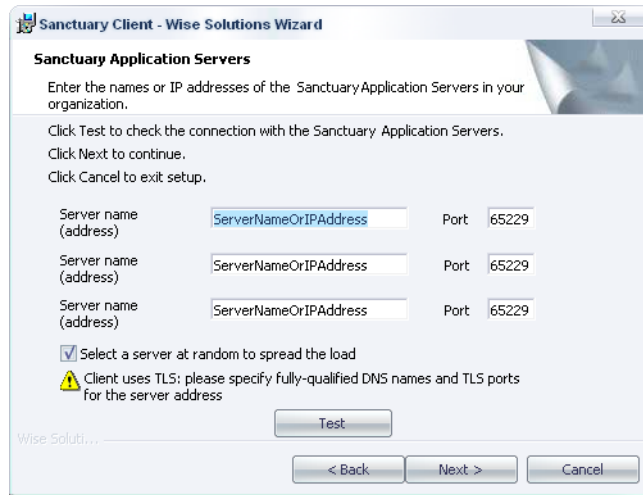


**Figure 6.6** Sanctuary Client: Certificate's parameters

7. Enter the *Server name* of at least one Sanctuary Application Server on your network. You can enter up to three server names during the setup and more afterwards in the client registry (see [Appendix B, "Registry Keys"](#) on page 153 for details). The dialog accepts fully qualified domain names (FQDNs) or IP addresses. If you are using TLS protocol, you **MUST** specify



fully qualified DNS names for the servers. You can also proceed without providing a server address.



**Figure 6.7** Sanctuary Client: Sanctuary Application Server name or address

8. Click on the TEST button to check that the Sanctuary Client can establish a connection with the Sanctuary Application Server(s) listed. A test is considered successful if the computer is online, a Sanctuary Application Server could be contacted, and the key pair match is correct. The ports are different if you are using TLS (65229) or not (65129). If using TLS, there is a REQUEST CERTIFICATE button that is used to contact the Certificate Authority and ask for a valid computer certificate.

There are three different cases:

- You specify a correct address for the Sanctuary Application Server. This address is validated and, if correct, the setup continues. All permissions for the client are retrieved from the server(s) specified in this dialog.
- You specify a momentarily unavailable address, invalid address, or no address at all. The setup continues after warning you. You can use this mode to deploy the Sanctuary Client on machines that are not currently connected to a Sanctuary Application Server, but you want or need to apply predefined permissions (devices and/or executables) that should be immediately activated after the setup ends. In this latter case, you also need to generate the *policies.dat* file (see your corresponding *Administrator's Guide*). If this file is not available, the default built-in restrictive settings are applied.
- There is a valid server and the *policies.dat* file exists, policies are imported from this file.

**Table 6.1** Server address and import file relationship

Sanctuary Application Server address	Import file (Policies.dat)	Resulting action
Valid and reachable	Not present	The settings are taken from the server.
Valid and reachable	Present and valid*	The settings are taken from policies.dat.
Valid but not reachable, no address provided, invalid address	Not present	The settings are the predefined ones (most restrictive — see notes and warning below) until a server can be contacted and the permissions updated.
Valid but not reachable, no address provided, invalid address	Present and valid*	The settings are taken from the policies.dat file until a server can be contacted and the permissions updated.
*The policies.dat file has a validity period of 14 days after generation (default value)		

By default, the driver randomly chooses an available server to work with. This setting allows the load to be shared between available Sanctuary Application Servers. If a server is unavailable, the driver picks up another one from the list and tries to connect to it.

You can also choose to contact the servers sequentially in the order you enter them. This setting is ended for particularly adapted to configurations that have a primary Sanctuary Application Server and a backup one. The driver connects to the primary Sanctuary Application Server, that is, the first one on the list, unless this is not available, in which case the driver tries to connect to the next one on the list.



**Warning:** If you are installing Sanctuary Device Control and there is no Sanctuary Application Server to contact or exported policies to use, the most restrictive policies apply. The client has no permissions at all even when some devices have predefined restricted permissions, for example, read/write permissions for the PS/2 port. See the Sanctuary Device Control User Guide for a list of the predefined permissions when first installing the program.





**Warning:** If there is no Sanctuary Application Server to contact or exported policies to use and you are installing Sanctuary Application Control Suite, applications are NOT blocked until the first contact has been established.

- 9. Choose between spreading the load through all selected servers (random load balancing) and selecting them in the order provided in the fields. To do this, activate (or deactivate) the *Select a server at random to spread the load* option.
- 10. Click on NEXT to proceed. The server address is validated, but you can still continue if it is invalid or unspecified:

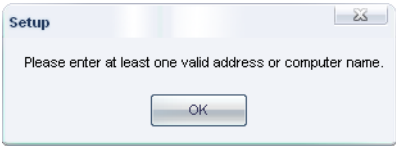


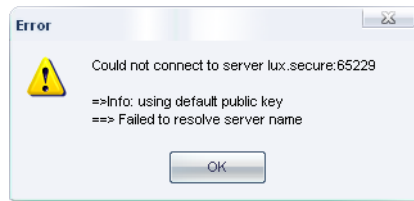
Figure 6.8 Sanctuary Client: No address specified



Figure 6.9 Sanctuary Client: No valid address specified or cannot contact server

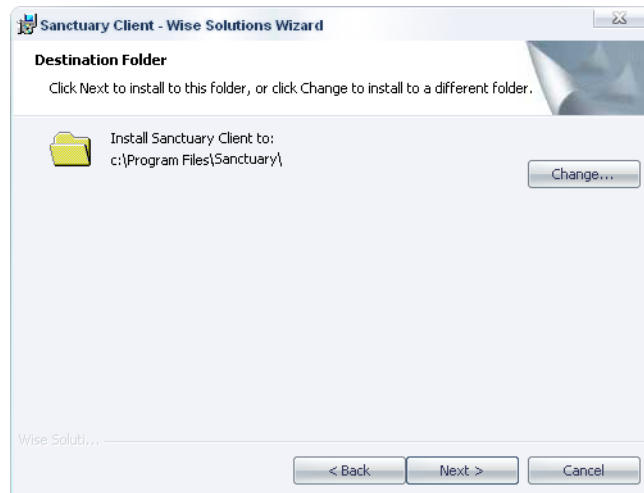






**Figure 6.10** Sanctuary Client: Test failed

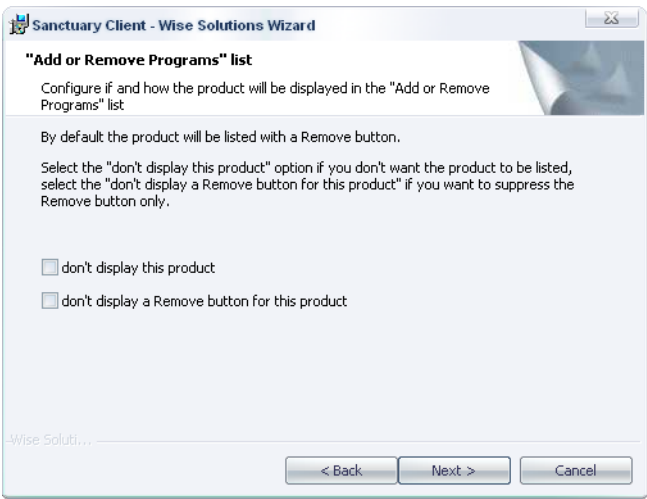
11. Choose the target directory for the installation and click on NEXT to continue.



**Figure 6.11** Sanctuary Client: Change the target directory



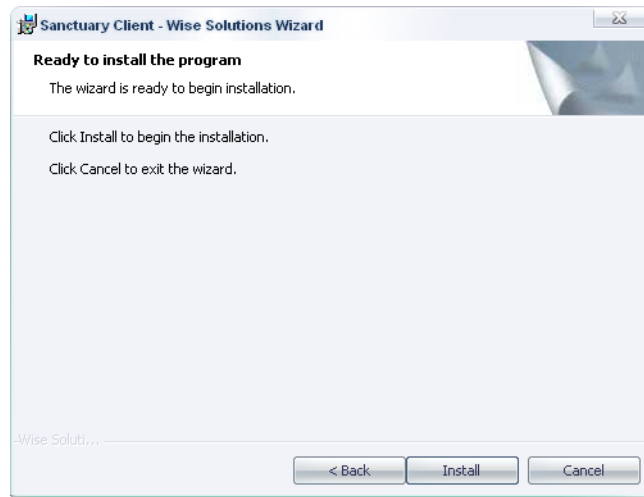
12. Choose how the uninstall process is controlled. You can select the first option so that the program is not listed on Windows' *Add Remove Programs* dialog or select the second one to show the program in the list but not provide a REMOVE button:



**Figure 6.12** Sanctuary Client: How will the program appear on the Windows' Add Remove Program dialog

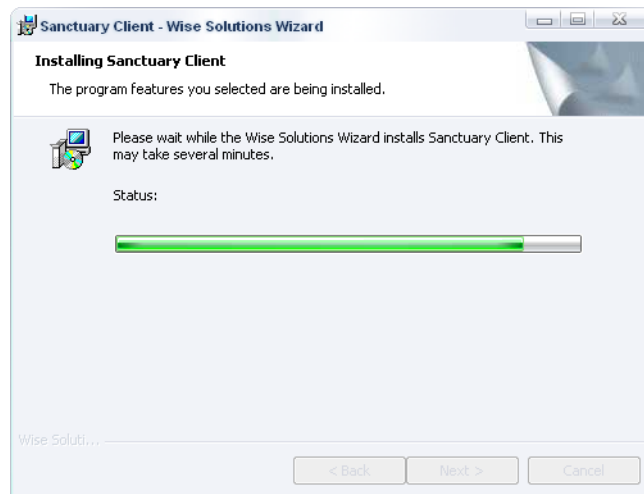


The program is now ready to be installed:



**Figure 6.13** Sanctuary Client: The installation process is ready to start

13. Click on **INSTALL** to proceed. The setup takes about 2 minutes, depending on the hardware in use.



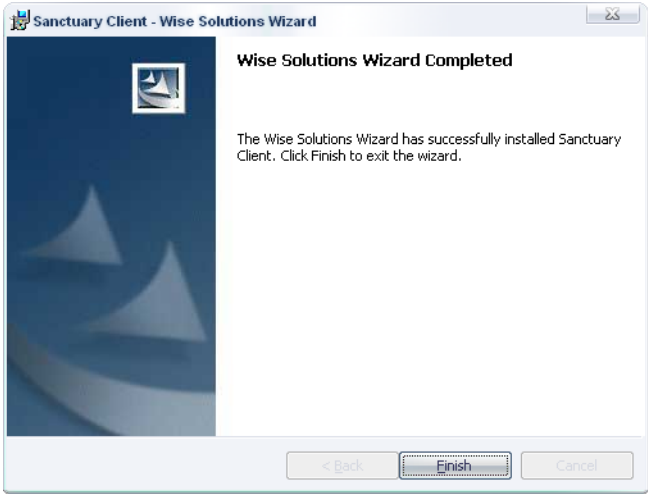
**Figure 6.14** Sanctuary Client: The installation progress





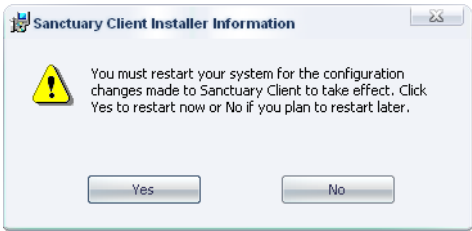
**Note:** You may also see an error message if you are using Windows XP SP2 or later and the TCP port that the firewall blocks cannot be unblocked by the installation program.

- 14. Click on FINISH to close the dialog and complete the procedure.



**Figure 6.15** Sanctuary Client: Finishing the installation process

- 15. Reboot your computer when prompted to do so by the Sanctuary Client setup program. To do this, click on YES to restart the computer.



**Figure 6.16** Sanctuary Client: Restarting the computer





**Note:** It is not recommended to delay rebooting and continue working. Doing this may result in a network or application instability.

The following dialog is displayed if the policies file could not be retrieved or initialized. If you choose to ignore this situation, you risk blocking your machine since the most restrictive of all policies applies — i.e. no device access at all.



**Figure 6.17** Sanctuary Client: No import file and no server address specified



**Warning:** If there is no Sanctuary Application Server to contact or exported policies to use and you are installing Sanctuary Application Control Suite, applications are NOT blocked until the first contact has been established.



After finishing the installation, you now have all the required components copied in the selected installation folder, several directories created, and all the required registry keys generated in the client machine.

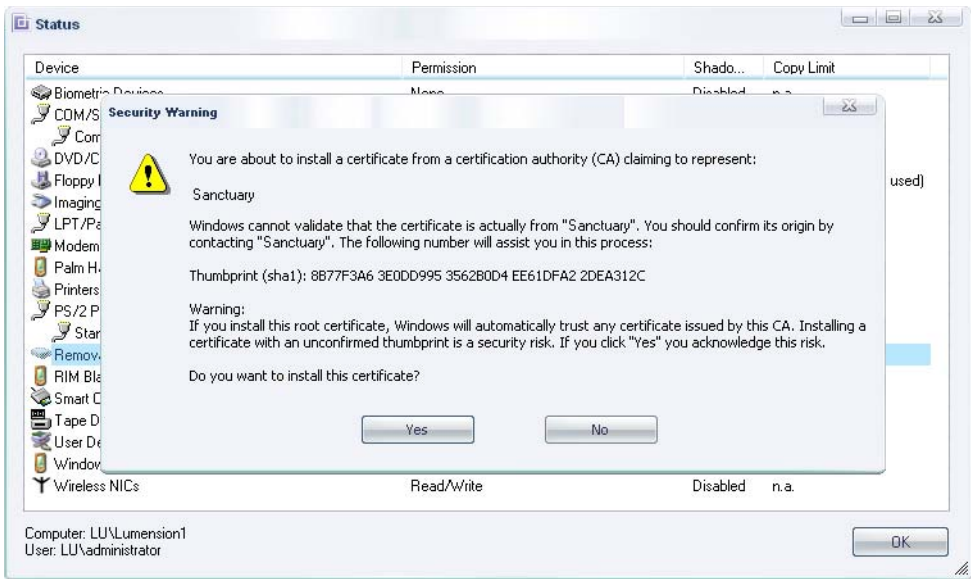


Figure 6.18 Sanctuary Client: Certificate generation and installation

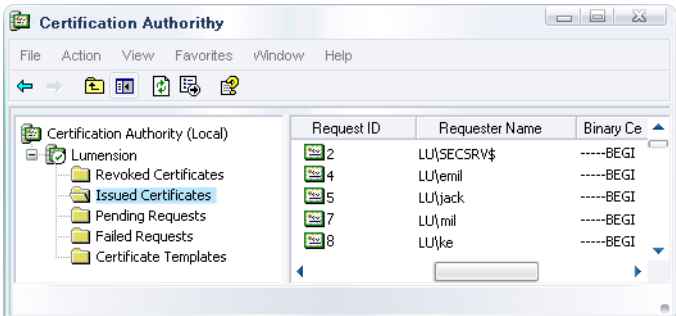


Figure 6.19 Sanctuary Client: Certificate Authority issued certificates



## Unattended Installation of the Sanctuary Client

---

Once you have installed and tested your Sanctuary software configuration on a few computers, you will want to deploy it on all or most of the computers on your network. See [Chapter 8, “Unattended Client Installation”](#) on page 93 for information about how to do this without having to physically visit each client computer and run the Setup program.

## Uninstalling the Sanctuary Client

---

At any time after installing Sanctuary Client, you can uninstall it from the client computer. If you used Group Policy to do an unattended installation, then you can also use Group Policy to uninstall the client(s).



**Note:** Uninstalling the Sanctuary Client briefly disconnects the computer from the network. This behavior can cause problems if you are working in a remote connection or doing other remote tasks.

You can use the Client Deployment Tool to do an unattended install/uninstall of the client package. See [“Using the Sanctuary Client Deployment Tool to Install the Sanctuary Client”](#) on page 106 .

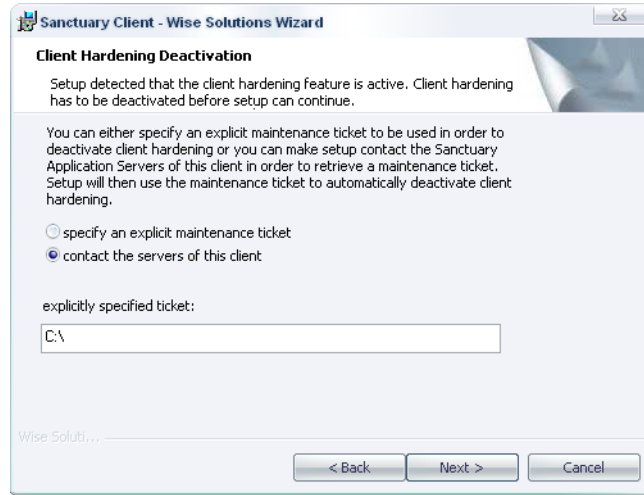
If the client was installed manually, then select Add/Remove Programs from the Windows Control Panel, and choose Sanctuary Client from the list of installed programs. The Setup program launches and uninstalls Sanctuary Client. You must reboot the computer once finished. Remember that this option may or may not be present, depending on choices you made during the setup process.



**Tip:** If a network shared disk was used during the initial installation, and this disk is no longer available during uninstall, the MSI program may ask specifically for the original setup file location before it can continue. A workaround solution for this problem is to copy the original MSI setup file on the local hard drive, then point the MSI uninstaller towards this file. You can remove the MSI setup file from the local hard drive once the client is deleted.



Since you are now in a highly secure environment and client hardening is enabled, changes to the client and its components have to be done in an orderly fashion. Even if you are an administrator, the services, registry entries, and special directories of the client cannot be modified before taking some measures to certify that you have the right to do so.



**Figure 6.20** Defining from where does the Sanctuary Client gets its maintenance ticket

To uninstall the client you should either:

- Deactivate the ‘client hardening’ option using the management console.
- Generate an ‘Endpoint Maintenance Ticket’ that overrules the ‘client hardening option’.

If you chose to create and save an endpoint maintenance ticket, the client will search for it:

- On the same directory where the .msi package resides (‘default maintenance ticket’ called ‘ticket.smt’).
- In the ‘ticket’ directory which is created by the setup during the client installation (‘explicit maintenance ticket’).
- Request it from a Sanctuary Application Server (the user must have valid credentials to do this) if you are using our client deployment tool.

Please consult your corresponding *Administrator’s Guide* or help file for a complete description on how to create an Endpoint Maintenance Ticket.



## Load Balancing Methods

---

### What is Load Balancing

When you have two or more Sanctuary Application Servers in your network, it is necessary to distribute the processing activity evenly so that the Sanctuary Application Servers work in a more or less 'balanced' state and no single server is overwhelmed. Load balancing is especially important when it is difficult to predict the number of requests that will be issued to a server.

One approach is to use a load balancing technique called round robin, which works on a rotating basis, i.e. in a loop.

### How Does Round Robin DNS Works?

When a DNS server that is configured in a round robin fashion receives a request, it resolves the name to one of the available IP addresses stored in its table in a rotated order. This redirects the request to one of the Sanctuary Application Server in the group.

As an example, and using [Figure 6.21](#), on page 82 as reference, when the first request arrives at the DNS server, it returns IP address # 192.168.1.1, the first machine. On the second request, IP address # 192.168.1.2. And so on. Assuming that we only have three servers defined in the DNS table, on the fourth request, the first IP address is returned once more.

Using the above DNS round robin schema, all of the requests sent to Sanctuary Application Servers have been evenly distributed among all of the machines in the cluster. All of the nodes in the cluster are exposed to the clients.

### Advantages of DNS Round Robin

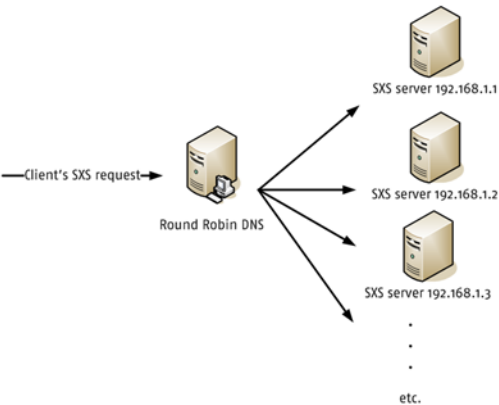
Although very easy to implement, round robin DNS has some drawbacks, such as inconsistencies in the online DNS tables when remote servers are unpredictably unavailable. However, this technique, together with other load balancing and clustering methods, can produce good solutions in many situations.

The main advantages of DNS round robin are:

- **Inexpensive and easy to set up.** The system administrator only needs to make a few changes in the DNS server to support round robin. Clients are not even aware of the load-balancing scheme they are using.
- **Simplicity.** You can add or remove servers as you go. All clients are identically installed using only one DNS alias provided as a Sanctuary Application Server.



When servers are added or removed, you only need to edit one DNS table, not to modify registry settings.



**Figure 6.21** Round Robin DNS schema

**Note:** Windows 2000 has some bugs related to DNS round robin. You must apply the latest patches solves them.



## Items Created During the Sanctuary Client Setup

When doing a Sanctuary Client installation, the setup creates the following items:

**Table 6.2** Items created by a Sanctuary Client installation

Item	Purpose	Access
Directory: %INSTALLDIR%\Client	Contains the Sanctuary Client and all required components.	Restricted access granted to Administrators and LocalSystem, read/execute access granted to Everyone. The security settings are propagated to child objects.
Directory: %INSTALLDIR%\Import	Used for a special file that is used to import permissions. This file is created by exporting permissions using the Sanctuary Management Console and has a two-week validity.	Read/write access granted to Everyone.
Directory: %INSTALLDIR%\Ticket	Where the endpoint maintenance ticket has to be copied in order to relax 'client hardening'.	Read/write access granted to Everyone.
Directory: %SYSTEMROOT%\SXData	Contains several files that are required for the program to work.	Restricted access granted to Administrators and LocalSystem. The security settings are propagated to child objects.
Directory: %SYSTEMROOT%\SXData\shadow	Contains the write/read shadow data (if necessary and defined by Sanctuary's Administrator).	Inherits its security settings from %SYSTEMROOT%\SXData.
Registry keys*: HKLM\system\CurrentControlSet\Services\scomc\parameters — and — HKLM\system\CurrentControlSet\Services\sk\parameters	Registry keys. See <a href="#">Appendix B, "Registry Keys"</a> .	n/a
*You can block the use of the RegEdit.exe program for all users by using our Sanctuary Application Control Suite component.		



**Note:** The %INSTALLDIR% directory points to the folder where the program was installed. It is usually C:\Program Files\Lumension Security\Sanctuary, but can refer to another folder. %SYSTEMROOT% is usually C:\Windows.





# 7 The Sanctuary Authorization Service Tool

Software Update Services (SUS) assists Microsoft Windows administrators with the distribution of security fixes and critical update releases provided by Microsoft. It distributes official updates to Microsoft Windows 2000, XP, and 2003 computers, including servers and desktops. Using SUS is equivalent to running Windows Update service within your own network.

Windows Server Update Services (WSUS, previously SUS v2.0) is a new version of Software Update Services (SUS). WSUS supports updating Windows operating systems as well as all Microsoft corporate software (like Office and SQL).

The information in this chapter applies only to the Sanctuary Application Control Suite (Sanctuary Application Control, Sanctuary Application Control Server Edition, or Sanctuary Application Control Terminal Services Edition).

## What is the Sanctuary Authorization Service Tool?

You can use *Sanctuary Authorization Service Tool* (AuthSrv.exe) to monitor changes on the approved and synchronized files done by SUS or WSUS, and process them, when needed, using our *Versatile File Processor Tool*, 'FileTool.exe' (see the *Sanctuary Application Control user Guide* for more information). The aim of this process is to require 'zero' administration effort, i.e. all Microsoft Authorized updates and fixes are automatically approved, their Hash created, and the database updated. See the configuration details in the *Sanctuary Application Control User Guide*.



**Note:** Notice that we do not support either Outlook Express or Internet Information Server (IIS) as clients for sending email messages. If there is already an account in these types of clients, the SMTP IP address is transferred directly to the AuthSrv configuration. Furthermore, the 'LoadConfiguration' registry key parameter is always set to '3' (see the Sanctuary Application Control User Guide).



**Note:** SUS does not support Windows Vista.

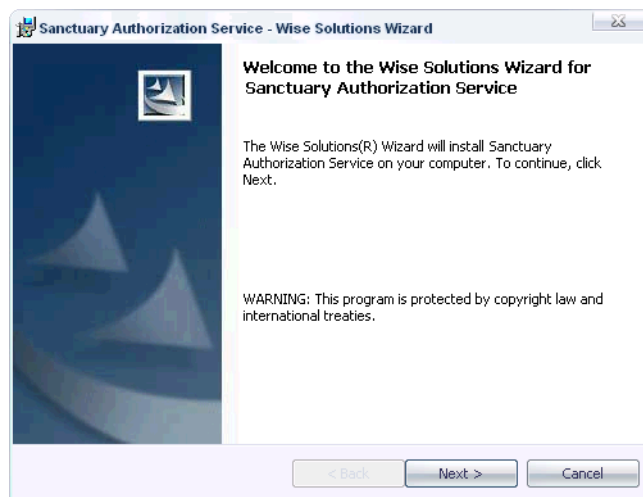


### To Install the Sanctuary Authorization Service Tool

---

The installation of the Sanctuary Authorization Service Tool (AuthSrv.exe) is done through a setup Wizard. To install the tool follow these steps:

1. Localize and run the installation wizard on the Sanctuary CD (server\AuthSrv\Setup.exe). The welcome screen is shown:

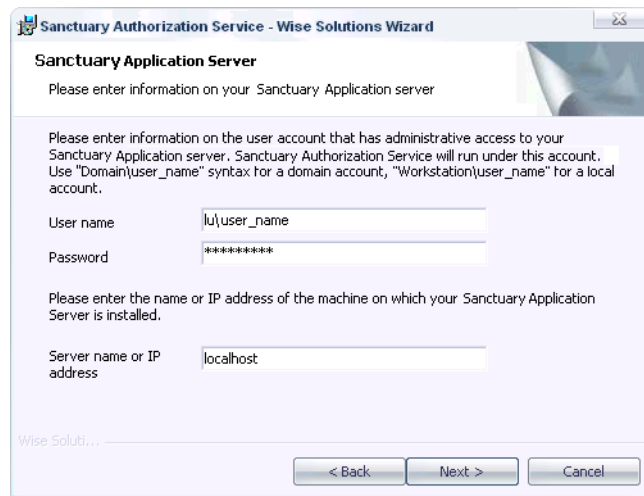


**Figure 7.1** Sanctuary Authorization Service Tool installation: Welcome screen

2. Click on NEXT. The License Agreement is shown.
3. Read the license agreement carefully and, providing you agree with its conditions, select the accept option and click on NEXT.

If you do not agree with its stipulations, click on the CANCEL button to exit without installing the Sanctuary Authorization Service Tool.

4. Enter the user's name and password, the Sanctuary Application Server IP or name and click on NEXT to continue.



The image shows a Windows-style wizard window titled "Sanctuary Authorization Service - Wise Solutions Wizard". The window has a light blue header bar with the title and a close button. Below the header, the main content area has a light blue background. The title "Sanctuary Application Server" is displayed in bold. Below it, the text "Please enter information on your Sanctuary Application server" is shown. A small graphic of a document with a pencil is on the right. The main instructions read: "Please enter information on the user account that has administrative access to your Sanctuary Application server. Sanctuary Authorization Service will run under this account. Use 'Domain\user\_name' syntax for a domain account, 'Workstation\user\_name' for a local account." There are three input fields: "User name" with the placeholder text "lu\user\_name", "Password" with placeholder text "\*\*\*\*\*", and "Server name or IP address" with the placeholder text "localhost". At the bottom, there are three buttons: "< Back", "Next >", and "Cancel". The text "Wise Soluti..." is partially visible at the bottom left.

**Figure 7.2** Sanctuary Authorization Service Tool installation: Configuration screen



5. Configure the SUS and Sanctuary Authorization Service Tool to suit your requirements and click on NEXT.

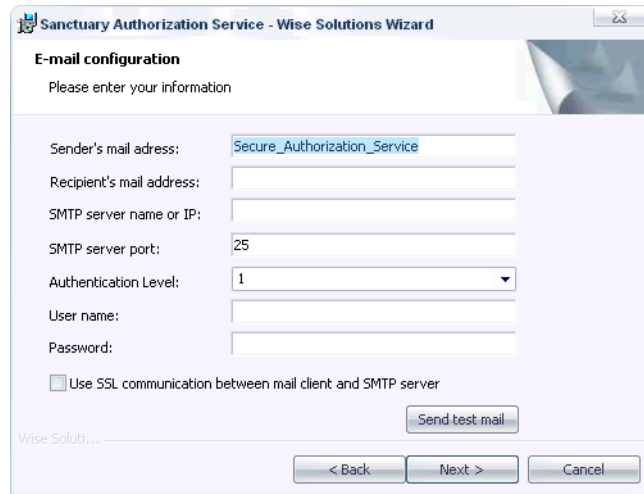


**Figure 7.3** Sanctuary Authorization Service Tool installation: Option screen

6. If you selected the e-mail option in the previous step, configure this by completing the corresponding fields and click on NEXT.



The program creates a test e-mail. If the send action is successfully finished, you get a message informing you that the test has been sent and everything is working correctly.

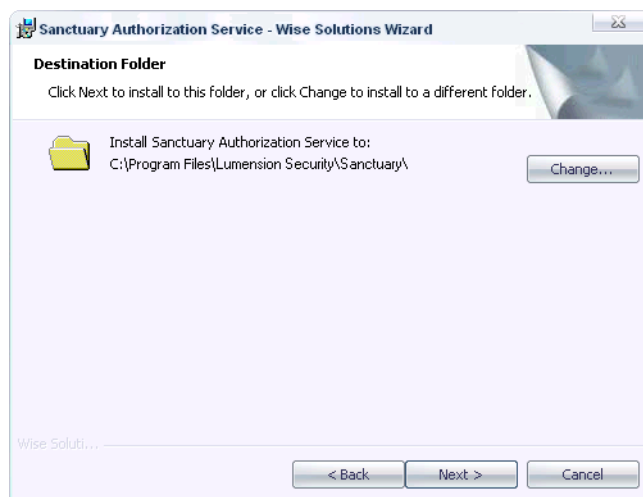


The image shows a Windows-style wizard window titled "Sanctuary Authorization Service - Wise Solutions Wizard". The window has a light blue header bar with a small icon on the left and a close button on the right. Below the header, the title "E-mail configuration" is displayed in bold, followed by the instruction "Please enter your information". The main area contains several input fields: "Sender's mail address:" with the text "Secure\_Authorization\_Service" entered; "Recipient's mail address:" (empty); "SMTP server name or IP:" (empty); "SMTP server port:" with the value "25"; "Authentication Level:" with a dropdown menu showing "1"; "User name:" (empty); and "Password:" (empty). Below these fields is a checkbox labeled "Use SSL communication between mail client and SMTP server", which is currently unchecked. To the right of the checkbox is a "Send test mail" button. At the bottom of the window, there are three buttons: "< Back", "Next >", and "Cancel". The text "Wise Soluti..." is partially visible at the bottom left of the window.

**Figure 7.4** Sanctuary Authorization Service Tool installation: E-mail configuration screen



7. Accept or change the installation directory (the program proposes `c:\Program Files\Lumension Security\Sanctuary`) and click on NEXT.



**Figure 7.5** Sanctuary Authorization Service Tool installation: Choose installation directory

The final summary screen is shown. You are now ready to install the program.

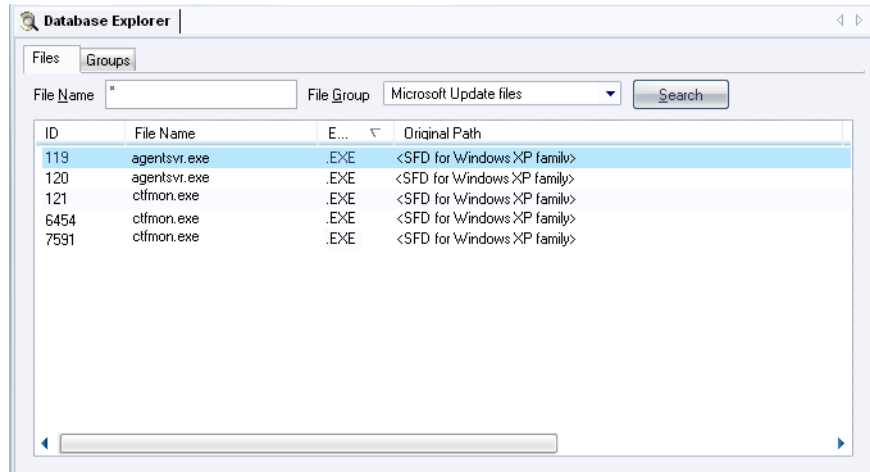
8. Click on NEXT, BACK to change options, or CANCEL to stop the setup. You will see the progress window and the final screen.
9. Click on the FINISH button to close the setup window.

If you did not activate the *Do not automatically start the Sanctuary Authorization Service Tool when Setup is finished* option, the program starts once the installation ends.

The tool waits until:

- A change is made in the default update folder by WSUS.
- The administrator approves the updates on the SUS console.
- Each hour.

- Once installed and loaded, you get a screen similar to that of [Figure 7.6](#) when choosing *Microsoft Update Files* in *File Group* field of the Database Explorer module of the console (assuming you have some update files ready to authorize):



**Figure 7.6** Sanctuary Authorization Service Tool initial scan

## Configuring WSUS

Once the Sanctuary Authorization Service Tool has been installed, you must configure the WSUS system since this tool does not support express (.msp) installation files. To do this:

1. Open Internet Explorer with your WSUS server active ([http://<server\\_name>/WSUSAdmin](http://<server_name>/WSUSAdmin)).
2. On the WSUS console toolbar, click on **OPTIONS**, and then select **SYNCHRONIZATION OPTIONS**.
3. Under the **UPDATE FILES AND LANGUAGES** section, click on **ADVANCED** and accept the warning message by clicking on **OK**.
4. Deselect the *Download express installation files* checkbox.



If you want to reactivate them, follow the same procedure and click on the *Download express installation files* option.

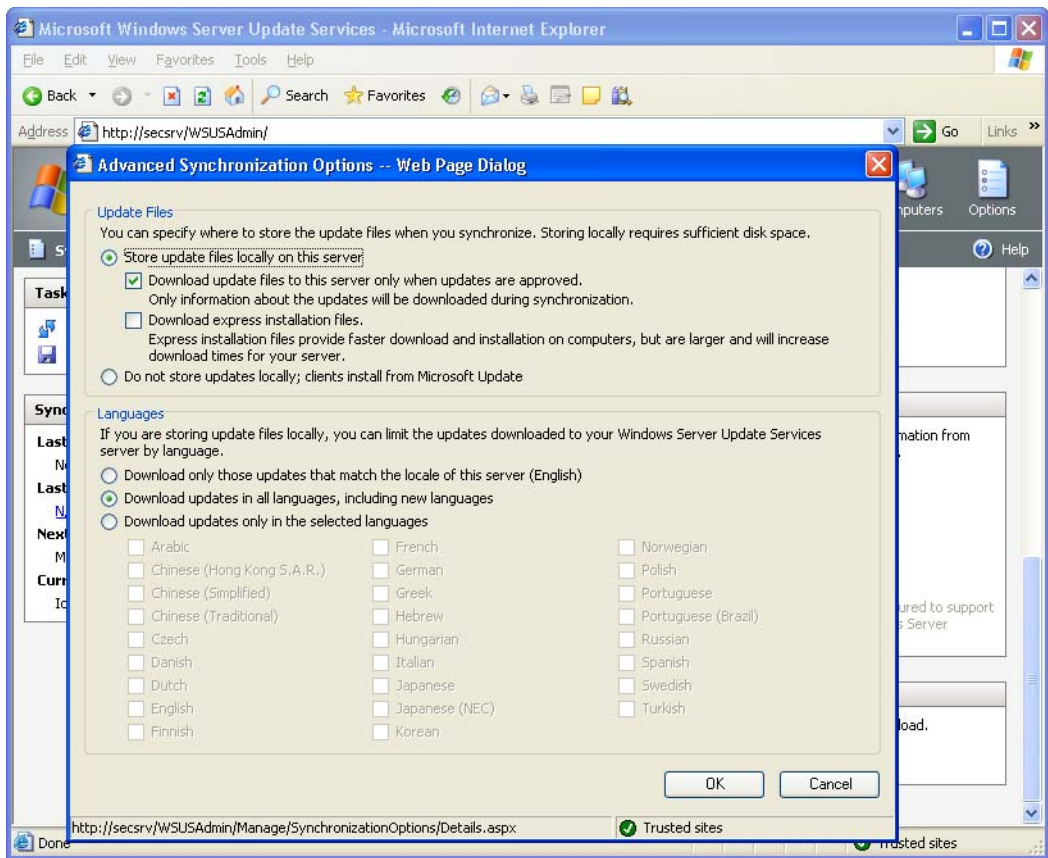


Figure 7.7 WSUS configuration



## 8 Unattended Client Installation

Once you have installed and tested your Sanctuary configuration on a few computers and are satisfied that you can administer it effectively, the next step is to deploy it on all or most of the computers on your network. If you have a large number of computers to manage, this is made much simpler with an unattended installation. This is also the easiest way of ensuring that all computers have the correct package. In addition, you can use our tool to obtain a list of all machines that already have the client deployed.

This chapter explains how to install the Sanctuary Client using MSI technology and optionally Windows 2000/2003 Group Policy. The information in this chapter is relevant to all Sanctuary software suite products.



**Warning:** If you prefer to use a different deployment tool, you should be aware that some of them, by design limitations or errors in their configuration, do not do a completely 'silent' installation and sometimes fail since they are waiting for user input.



**Warning:** If you are using encrypted communications using the automatic certificate generation mode, the client deployment task cannot be successfully completed unless you guarantee that the machine certificate file's properties (located at %SystemDrive%\Documents and Settings\All Users\Application Data\Microsoft\Crypto\RSA\MachineKeys) are 'Full Control for Administrators and LocalSystem' (the usual setting).



**Note:** If you are installing Sanctuary Device Control or Sanctuary Application Control on Windows XP SP3 or Vista machines, you need to open certain blocked ports to be able to do an unattended client installation. See [Appendix E, "Opening Firewall Ports for Client Deployment"](#) on page 181 for more details.



**Note:** You cannot install Sanctuary Application Control Server Edition client on Windows XP, 2000 Pro, or Vista machines.





**Note:** Although the installation dialog only lets you input three Sanctuary Application Servers, you can easily add more if needed. You can also change how the Sanctuary Application Server(s) is selected — round robin vs. random pick. All this is done by modifying certain registry keys. See [“Sanctuary Client Registry Keys”](#) on page 163 and [“Uninstalling the Sanctuary Client”](#) on page 79 for more details. You can ‘push’ these modifications to all clients using Group Policies with ADM templates.



**Note:** The client setup package is available for 32-bit and 64-bit operating systems. If you create an installation package that includes the 32-bit client and try to install it on a machine with a 64-bit OS, the installation will fail and rollback. The same is true the other way around. If you are working on a mixed environment containing both 32-bit and 64-bit machines, you should create two distinctive installation packages, one for each type of OS.

Even though you can use other deployment packages to install Sanctuary Client, our specialized silent unattended installation deployment tool offers you the advantage of doing (among other things):

- Port unblocking.
- Policy import.
- Standalone client installation and licensing.
- Import client communication layer parameters.
- Generated public key installation.
- Removal of obsolete data files.
- Client hardening detection and, if required, deactivation.
- Client communication layer’s Windows Management Instrumentation (WMI) interface registration.
- Installation of WMI redistributable components.

The installation process is carried out in five stages:

1. The original client’s setup MSI file is used as the base for a client deployment. This file is copied to whatever directory you choose when you first start the Sanctuary Client Deployment Tool tool. After deciding on a name for your installation package, a new folder is created using this name. For example, if you want your installation packages to be located in a directory named ‘Deploy’ and the installation package name is ‘Marketing’, the program places the client MSI file in C:\Deploy\Marketing\.
2. After modifying the installation options, a new transform file (MST) is created in the installation package folder.

3. The license, policies (optionally), and public key files are copied (exported) to the same folder where the MSI and MST files reside.
4. The computer(s) on which the package will be installed are defined.
5. The deployment process is started.

## What is an MSI File?

---

An MSI file is a database with relationally linked tables and a set of files either inside or accompanying it. This database contains information about what has to be done to the target machine in order to install the application.

The installation process itself is controlled by a list of 'Actions'. Several such lists are predefined in the MSI standard. These can be adjusted by 'Custom Actions', performing special tasks not covered by the normal MSI behavior. Custom actions can even launch scripts and executables to perform special installation tasks.

The actual installation process is performed by a special MSI installer service running on the computer. Because this service runs with system privileges, it has all the rights necessary to perform the installation. Depending on the local security policy, normal users can be granted the right to make the installer service install certain packages or even any package the user wants.

## Creating a Transform File (MST) for an Existing MSI File

---

Transform files are similar to MSI files but with a different file extension. They alter the installation process in order to encapsulate a set of required customizations. The contents of both MSI and MST files are merged together during the installation.

You can create MST files using a third party tool or directly with our Sanctuary Client Deployment Tool tool.

Since there are so many variables to control in the client MSI file, we strongly recommend using the Sanctuary Client Deployment Tool tool. In addition to the original MSI installation package, you now have an MST file with all necessary options to install on all your machines.

## Prerequisites for Creating a Sanctuary Client Deployment Tool Package

---

Before you create and install a deployment package, you must meet the following conditions:

- The administrator running the Sanctuary Client Deployment Tool tool must be in the Local Administrators group on all targeted computers. You can also use the command 'net use \\<computer>' to log on as an administrator.
- You must synchronize the clocks of the different computers. You can use Windows Time Service (W32Time, based on Simple Network Time Protocol or SNTP) to maintain date and time synchronization.



- If you are running the deployment tool on Windows XP SP2, check Microsoft Knowledge base article 884020 (<http://support.microsoft.com/default.aspx?scid=kb;en-us;884020> — Programs that connect to an IP address that are in the loopback address range) and, if necessary, install the provided patch.
- The deployment tool does not work under Windows NT4. **None** of Sanctuary's components are designed to work on this operating system.
- If there is a firewall between the Sanctuary Client Deployment Tool and the computer where you want to deploy the Sanctuary Client, open the following incoming ports on the client computers (see [Appendix E, “Opening Firewall Ports for Client Deployment”](#) on page 181):
  - TCP 33115.
  - TCP: 139, 445 NetBIOS.
  - UDP: 137, 138 Browsing.
- You must generate the key pair and have the public key available for the client. You also need the license file if you want to do a ‘standalone installation’ when using Sanctuary Device Control. If you plan to install on a client that does not have access to the Sanctuary Application Server, you also need to export the policies to a special file, *policies.dat*, and place it in the same client installation package.



**Note:** Installing a client using exported policies works well when policies.dat is placed locally in the same directory as setup.exe however if it is placed on a share you must change the security of the share directory so that computer accounts are able to access it.

- If you have already installed the client, using the client hardening feature, and want to uninstall/modify/repair it, you must first issue an ‘Endpoint Maintenance Ticket’ and copy it to the required directory. See the relevant *User’s Guide* for more information.

## To Install the Sanctuary Client Deployment Tool

---

The Sanctuary *Client Deployment Tool* tool is installed, among others tools, when setting up the Sanctuary *Management Console*. See [Chapter 5, “Installing the Sanctuary Management Console”](#) on page 53 for more information.

When considering the choice of the computer on which you install the Sanctuary Client Deployment Tool and from which you start the deployment, consider the following:

- The deployment of the Sanctuary Client on a long list of computers may take some time. You cannot log off the computer during that period.
- The tool makes significant use of the network resources of the computer on which you are installed.
- You must **NEVER** interrupt an ongoing deployment.



**Note:** If you wish to administer many machines at once with the deployment tool, use a server operating system like Windows 2000 Server or Windows Server 2003.



## To Install Packages

The installation process is carried out in the following two stages:

1. Create package(s).

The deployment tool allows you to select client installations (from the CD-ROM, LAN, or local drives). It makes a local copy of the client installation and displays the 'Options – Lumension Installation Transform' dialog so that you can create an installation transform (.MST) linked to the MSI file.



**Note:** An installation transform is a customization of the installation which predefines settings for the installed application. Having an installation transform allows the system administrator to apply identical settings to a group of client computers.

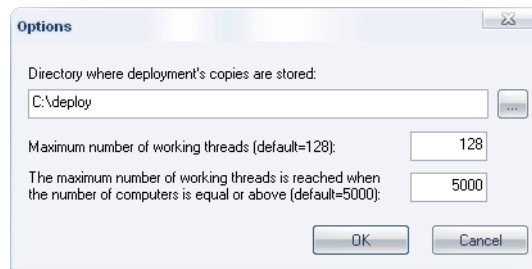
2. Install/Uninstall package.

To do this, select the package and target computer(s) to begin the (un)installation and set the reboot and configuration options. After this the deployment starts.

The following sections describe the installation process.

## To Install the Sanctuary Client: MST File Generation

1. On the administrator's machine, select *Sanctuary Client Deployment Tool* from the Start → Programs → Sanctuary menu. The following dialog appears on first use.



**Figure 8.1** Sanctuary Client Deployment Tool: First start-up

2. Choose the folder in which you would like to store all the deployment packages. You can modify this setting by using the *Options* entry of the *Packages* menu at a later point in time. Do not change other settings.





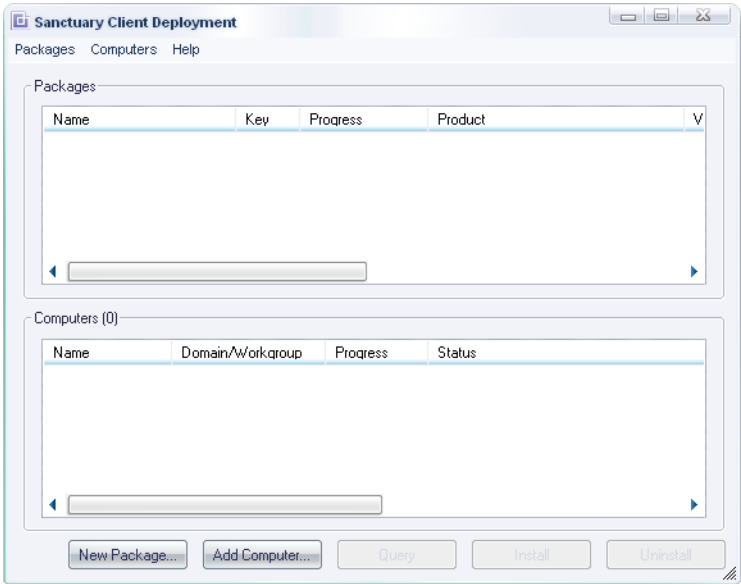
**Warning:** Do not specify the root directory of the system drive or any other directory where existing files already reside or might be created by other applications.

For a description of the other parameters see “[The Options Screen](#)” on page 130.



**Note:** If the deployment tool is installed on different machines, you may want to specify a shared directory where all instances of the deployment tool can access the company packages.

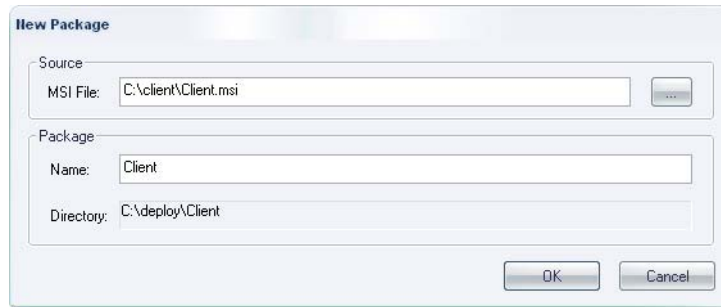
- 3. Click on OK. The following dialog appears:



**Figure 8.2** Sanctuary Client Deployment Tool: Packages and computers



4. From the *Packages* menu, select *New* or click on NEW PACKAGE (located in the lower part of the window). The following dialog is displayed:



**Figure 8.3** Sanctuary Client Deployment Tool: New package

5. Click on the ellipsis (⋯) button to select an MSI file, typically from the Client folder of the CD-ROM.
6. Enter the name you want to give to the package.

Do not use numbers in the form ###.###.###.### as they are interpreted as an IP address. Make a note of the directory (which we refer to as the Deployment package folder, C:\Deploy in this example).

7. Click on OK.



The installation files are copied to a subfolder of the destination directory as defined in step1 (C:\DEPLOY in our example). The *Options – Lumension Installation Transform* dialog is displayed:

**Figure 8.4** Sanctuary Client Deployment Tool: Sanctuary Application Server IP or name

- The two grayed-out options are only valid if you are installing older versions of our client:
- *Do not validate name or IP before installing.* Used to give a Server address or name that is not currently available but will be accessible afterwards.
  - *Enable wireless LAN protection.* An option available in older clients (v2.8 and before) that has now been superseded by permissions rules.
- On the other hand, the *Specify the policy import timeout (in minutes)* is only available for client version 3.2 or later (value between 20 and 100 minutes).



**Warning:** Although the Client Deployment Tool supports installing an older version of our client on Windows NT4, the tool itself does not work with this operating system.



8. Click on *Import public key*.
9. Select the `sx-public.key` file located in the `%SYSTEMROOT%\SXSDdata` folder of the Sanctuary Application Server machine.



**Warning:** If you do not find a `sx-public.key` file in the `%SYSTEMROOT%\SYSTEM32` or the `%SYSTEMROOT%\SXSDdata` (recommended location) folders of the Sanctuary Application Server, this means that your installation currently uses the default keys. You should not deploy clients in a production environment without having generated your own set of keys. See [Appendix 3, “Using the Key Pair Generator”](#) on page 29 for more details. Bear in mind if you are using Sanctuary Device Control that replacing an existing set of keys or implementing customized keys in an environment where encrypted media are already in use prevents recovering the password of these media.



**Note:** Although not recommended, it is possible to deploy the clients on test environments without a customized set of keys. If you do not want to generate custom keys, simply skip this step.



**Note:** The Sanctuary Client can be deployed without specifying a server address(s) that can immediately be validated. The server at the provided address(s) is contacted during the actual setup to make sure that the client can communicate with it. If this communication is not achieved, the installation is aborted unless the ‘Serverless Mode’ option is selected. See the following step for more information.

10. Enter the fully qualified domain names or IP addresses of the Sanctuary Application Server to which these clients attempt to connect, using the *Name or IP* fields. If alternative port numbers are required for these connections, then also type in the modified port numbers.

If you do not specify a fully qualified domain name or address, the installation is done in ‘*Serverless mode*’. While using this mode, the installation routine does not abort if it cannot reach a Sanctuary Application Server. Alternatively, if these fields are not empty, at least one Sanctuary Application Server must be contactable for the installation to continue, the install will rollback if all connection attempts fail.

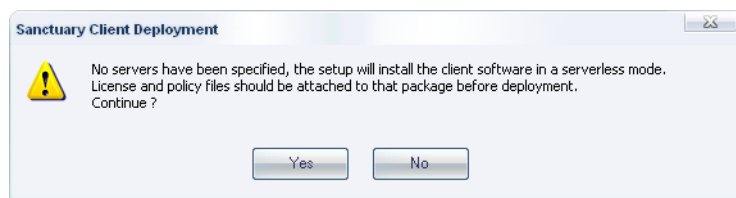
When installing in ‘*Serverless mode*’, you can also control policies by first exporting them to a special file (`policies.dat`) and you must include the license file. See [“To Install Sanctuary Clients”](#) on page 63 for details. If you are planning to do a client maintenance, it is important that the server(s) address are reachable since it is also used to retrieve the ‘Endpoint Maintenance Ticket’ needed to manage the clients (if installed in the Client Hardening mode) and its associated directories and registry keys. Please consult your corresponding *User’s Guide* and [“Uninstalling the Sanctuary Client”](#) on page 79 for more information.



The following list shows all the possibilities:

- Valid server, no policies file present  
Deploy succeeds using server information.
- Valid server: a valid policies file is present  
Deploy succeeds importing the policies file.
- Invalid server, no policies file present  
Deploy fails.
- Invalid server, a valid policies file is present  
Deploy succeeds importing the policies file (as soon as a server becomes available, it is used as the permissions/authorization source).
- No server found, no policies file present  
Deploy succeeds enforcing Sanctuary Device Control and/or Sanctuary Application Control permissions starting with the built-in restrictive policies (a valid Sanctuary license file has to be placed along with the .msi package) → ‘Standalone Installation’.
- No server found, a valid policies file is present  
Deploy succeeds importing the policies file → ‘Serverless Installation’.

When proceeding without specifying any servers, you get the following warning message:



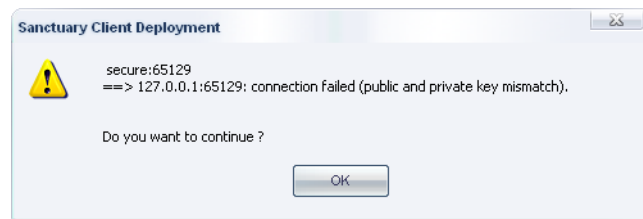
**Figure 8.5** Message when installing in ‘Serverless mode’

11. Choose whether to select the *Automatic Load Balancing* checkbox If you select this option, the Sanctuary Client attempts to contact one of the servers listed in a random manner. Alternatively, if you leave *Automatic Load Balancing* unchecked, the Sanctuary Client attempts to contact the Sanctuary Application Server in the order in which they are listed.
12. Choose whether or not the client uses TLS protocol to communicate with the Sanctuary Application Server. See “[Transport Layer Security](#)” on page 6 for more information.
13. Click on *Test Connection* to verify the fully qualified domain names or IP Addresses you have entered. A confirmation or failure dialog box is displayed.

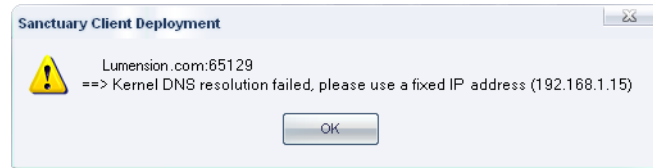
In the case of failure, check the error message for further details about the possible cause of failure (e.g. key pair mismatch, DNS resolution) and click on OK to continue. Here are some:



**Figure 8.6** Message when the connection test fails

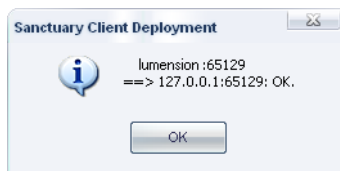


**Figure 8.7** Message when the connection test fails (key related)



**Figure 8.8** Message when the Kernel DNS resolution fails



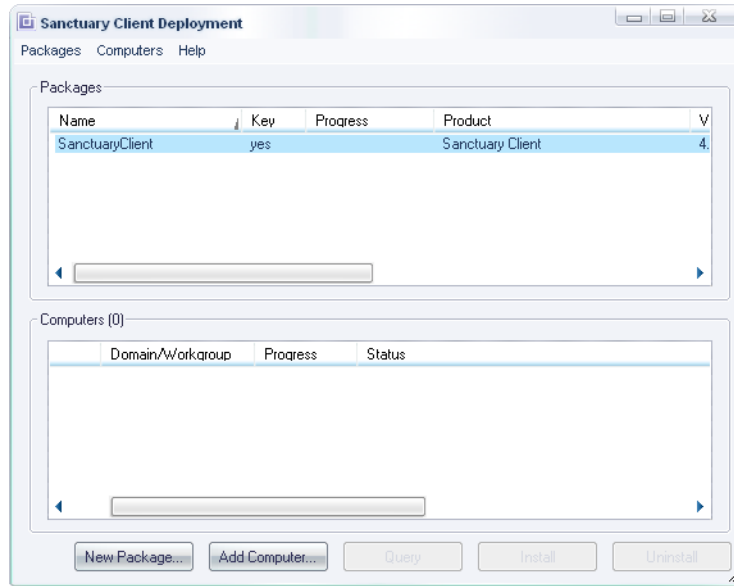


**Figure 8.9** Message when the connection test succeeds

14. Select the options that control how the client is shown in the *Add or Remove Programs* (Programs and Features in Windows Vista) Windows' dialog and the policy file timeout. The following options can be chosen:
  - *Suppress preventive actions...*: Since the client software depends on the licenses you own, it is possible to completely block a computer if you do not export correctly the policies ('Serverless' installation) or define them beforehand. This is especially true when installing our Sanctuary Application Control Suite and not authorizing those files belonging to the operating system. To avoid this, the program first verifies if there is an update from Sanctuary Device Control to Sanctuary Application Control Suite and that this action does not block the machine. If this is the case, the installation will not proceed and rolls back. Use this option if you do not want this check done and you are sure that you have correctly defined the policies.
  - *List the program with a 'Remove' button* – The program is listed in the 'Add or Remove Programs' (Programs and Features in Windows Vista) Windows' dialog in the 'standard' way, and it will include a *Remove* button.
  - *List the program but suppress the 'Remove' button* – The program is listed in the 'Add or Remove Programs' (Programs and Features in Windows Vista) Windows' dialog but will not include a *Remove* button.
  - *Do not list the program* – The program will not appear in the 'Add or Remove Programs' Windows' (Programs and Features in Windows Vista) dialog.
  - *Specify the policy import timeout (in minutes)* (only available for client version 3.2 or later) - set how many minutes should elapse before the program will consider the policy file as out of date. Type any value between 20 and 600 minutes (10 hours). You can use a value less than 20 minutes using the MSI installation file directly from the command line through parameters:  
`policy_import_timeout = <value_in_milliseconds>.`
15. Click on the OK button to close the dialog.



The new package appears in the Sanctuary Client Deployment Tool packages list:



**Figure 8.10** Sanctuary Client Deployment Tool: New package

A small file called 'Sanctuary Client.MST' is created in the Deployment package folder (C:\Deploy in our example). Select *Options* from the Packages menu to check the location of the Deployment package folder on your installation. The specified directory contains subdirectories corresponding to the packages you have just created.

You can see the options of each generated package in the main window:

Name	Key	Progress	Product	Version	Server(s)	Last deployment	License	Policies	TLS
client old versions	yes		Client	4.2.2	Secure	Install -01-11-2007 14h 37m 19s	yes	no	no
Client	yes		Client	4.2.2	192.168.1.1:65129		no	yes	yes
Special package	yes		Client	4.2.2			no	no	no

**Figure 8.11** Sanctuary Client Deployment Tool: Package option





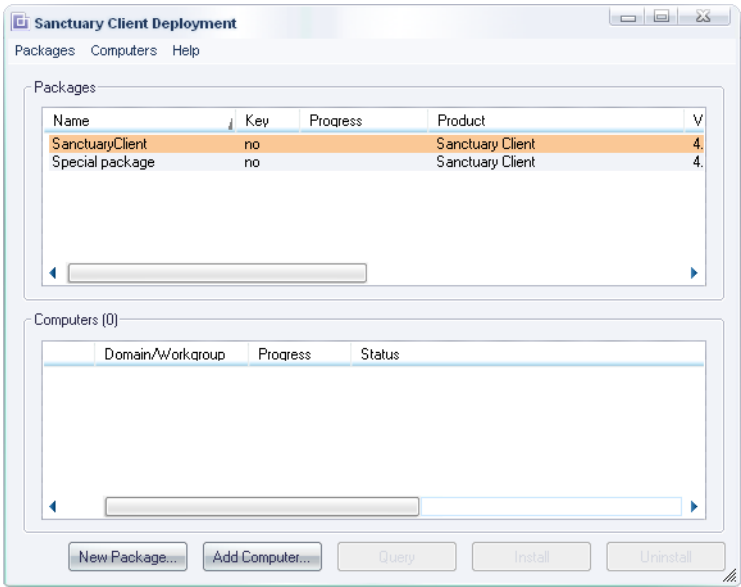
**Note:** If any of the public key, policies file, or license (in the case of an installation without servers), are not included in the package, they are displayed, as shown above, with an orange background as a warning. If there is no orange background, the key, policies file, and license, if applicable, are present and the package is ready to be deployed. We recommend you do not deploy packages without a public key — or license — in a production network. The license file is only required when doing a ‘Serverless installation’.

## Using the Sanctuary Client Deployment Tool to Install the Sanctuary Client

The Sanctuary Client Deployment Tool tool is designed to allow you to silently deploy the Sanctuary Client on a list of machines. Once the Deployment package has been created, you can start the deployment, using the following procedure:

1. Select *Sanctuary Client Deployment Tool* from the *Start → Programs → Sanctuary* menu.

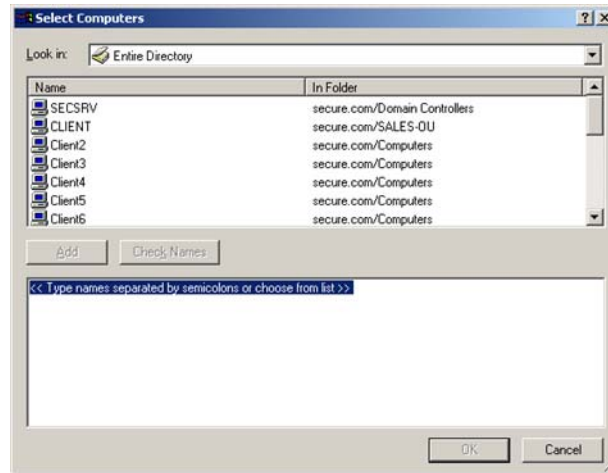
The Sanctuary Client Deployment Tool dialog is displayed:



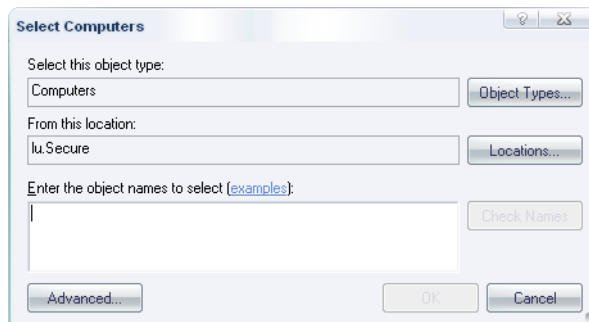
**Figure 8.12** Sanctuary Client Deployment Tool: First screen



2. Click on *Add Computer* (located in the lower part of the window) or select *Computer* → *Add* from the menu bar. One of the following dialogs is displayed, depending on your operating system:

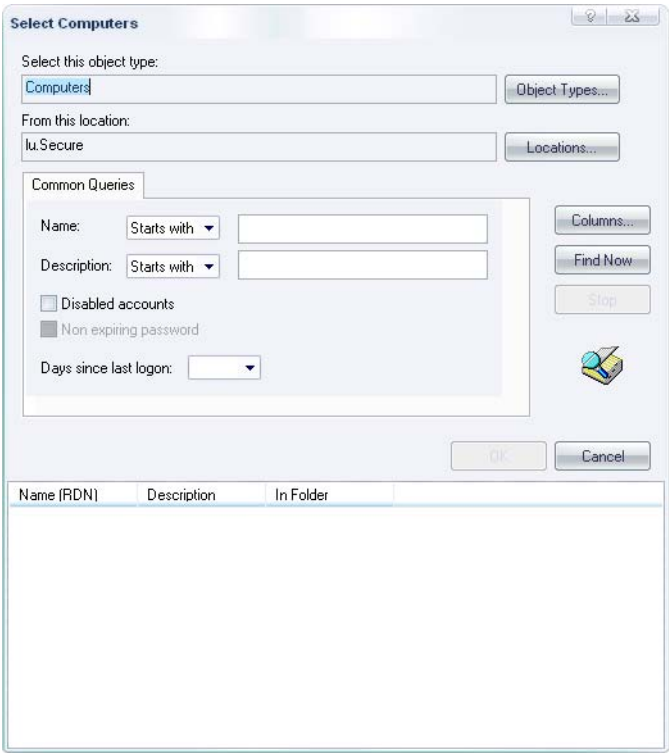


**Figure 8.13** Sanctuary Client Deployment Tool: Select computer dialog (Sample a)



**Figure 8.14** Sanctuary Client Deployment Tool: Select computer dialog (Sample b)





**Figure 8.15** Sanctuary Client Deployment Tool: Advanced select computer dialog

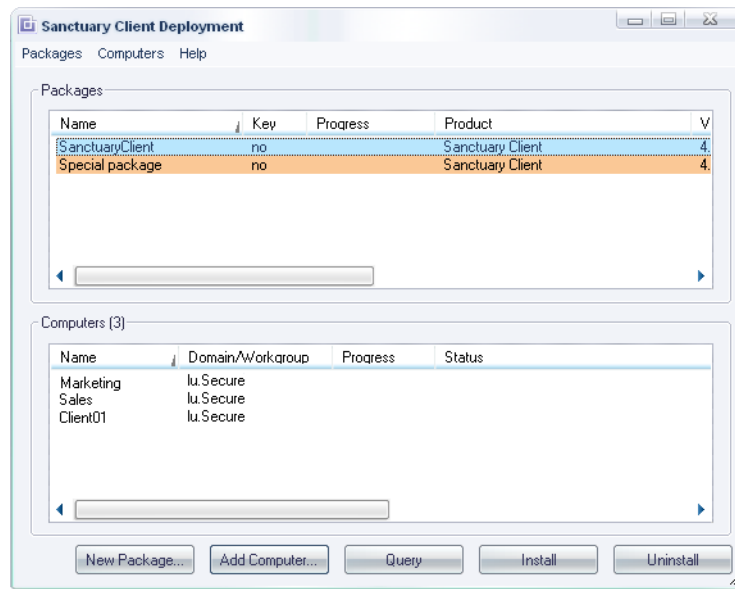


**Note:** You can also Drag and Drop between the external Microsoft Windows Network (from the My Network Places icon) selection dialog.

3. Select the domain you want to search and highlight (or enter) the names of the computers you want to add to the list. You can type in multiple names using a semicolon character ‘;’ to separate computer names.



4. Once you have selected the computers you want to add to the list, click on OK. The selected computers are now listed in the Sanctuary Client Deployment Tool dialog, as shown below.



**Figure 8.16** Sanctuary Client Deployment Tool: Selected computer(s)



**Note:** If the current or newer version of the client is already installed on a machine you select, it cannot be re-installed.



5. Choose whether or not the client will be communicating with the Sanctuary Application Server(s) using TLS protocol (see “[Transport Layer Security](#)” on page 6) and select the reboot options.



**Figure 8.17** Sanctuary Client Deployment Tool: Selecting the TLS protocol

To select TLS protocol, right click on a computer name and select CHANGE TLS MODE (or select it from the *Computers* menu).

When selecting the *Semi-automatic certificate generation*, you have the same options as those described for the client installation (described “[To Install Sanctuary Clients](#)” on page 63):

- Import — to place the machine certificate in the computer’s store.
- Select — to choose a certificate from the computer’s store.
- Advanced — to set the certificate’s cryptographic signature and parameters.

You must already have a Certificate Authority installed or the required computer certificate at hand. See [Appendix H, “Installing a Certificate Authority for Encryption and TLS Communication”](#) on page 203 for more details.

Remember that you also need an ‘Endpoint maintenance ticket’ if you are updating clients that require this type of permissions to be modified or updated. See your corresponding User’s Guide for a full description.



6. Select a register to install from the *Packages* list.
7. Optionally select a subset of machines where the package will be installed from the *Computers* list.
8. Click on INSTALL to start the deployment.

Sanctuary's administrator can decide to use a policy file, *policies.dat*, to export permissions to clients that are not connected, or cannot contact, to a server during the installation. See the *To export and import permission settings* section of the relevant *User's Guide* for more information about how to export your settings to a file.

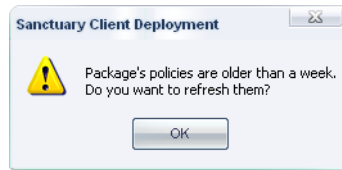


**Note:** If the installation detects an older version of the client, it will update it automatically.



**Note:** Installing a client using exported policies works well when *policies.dat* is placed locally in the same directory as *setup.exe* however if it is placed on a share you must change the security of the share directory so that computer accounts are able to access it.

If the exported policy file was created more than a week ago, you get the following message:



**Figure 8.18** Sanctuary Client Deployment Tool: Refreshing old policies file



**Note:** The policies file is valid for only two weeks (default value).

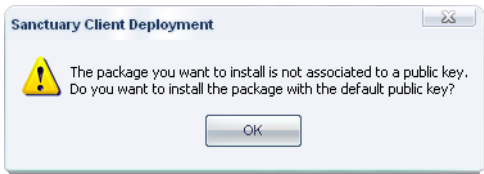


You can choose to either refresh the file or deny this request. If you choose to update these policies, you need to provide a Sanctuary Application Server valid address or name:



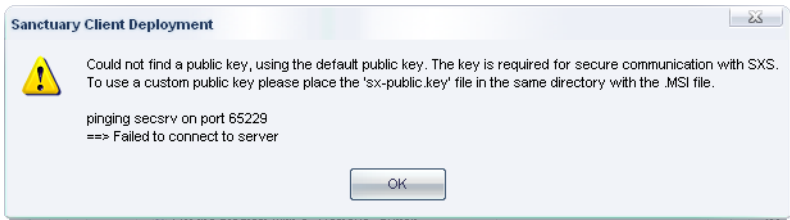
**Figure 8.19** Sanctuary Client Deployment Tool: Refreshing policies file

A similar scenario happens when you are not using a public key but are using the default one provided with the installation for testing purposes. Remember that it is not secure to communicate in a working environment with the default key; You should always generate a key pair when you install Sanctuary in a production machine. See [Chapter 3, “Using the Key Pair Generator”](#) on page 29 for more information.



**Figure 8.20** Sanctuary Client Deployment Tool: Missing public key during client deployment (1/2)

You can choose not to associate a public key pair with your client deployment (not recommended, see previous paragraph). If you click on **TEST CONNECTION** in the *Set Package Policies* dialog and you have not yet generated a public-private key pair, the following warning is displayed:



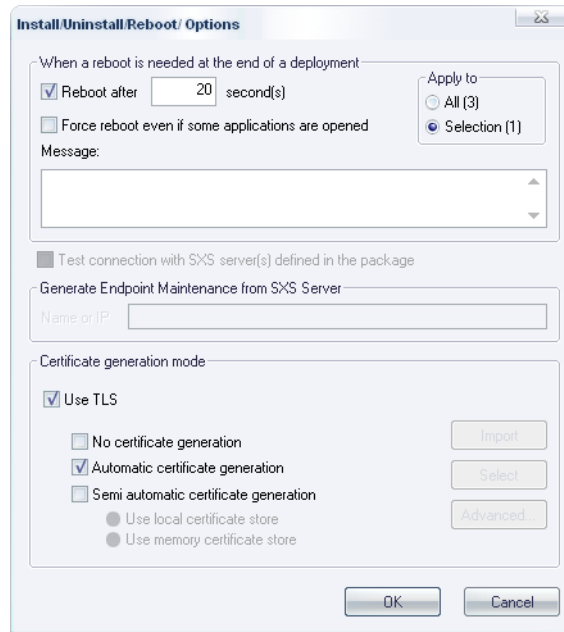
**Figure 8.21** Sanctuary Client Deployment Tool: Missing public key during client deployment (2/2)





You can also choose to import the public key — you should already have generated the key pair at this point. In this case, you should choose the file using Windows' *Open* dialog. Remember that you can always select to keep this file in an external device for added security.

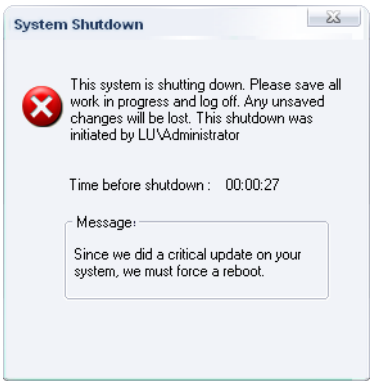
9. If the installation requires rebooting the client computers, the *Install/Uninstall/Reboot Options* dialog is displayed. If this is the case, select the appropriate options and click on OK. These options correspond to those already selected when creating the package.



**Figure 8.22** Sanctuary Client Deployment Tool: Reboot options



You can choose to require a reboot of the client computers after a defined period. You can also enter a text to be displayed to your users.



**Figure 8.23** Sanctuary Client Deployment Tool: Forced reboot message

If a subset of machines was selected from the *Computers* list, the *Apply to* options allow you to choose if you want to target only the selected set of computers (*Selection*) or the complete list (*All*).

The *Test connection with Sanctuary Application Server* option allows you to verify that the Sanctuary Application Server defined in the package is up and running before proceeding to the deployment on the client computers. It is a safe precaution to check this option unless you want to do an installation with no servers. See [“To Install Sanctuary Clients”](#) on page 63 for more information.

Specify the server name from where the ‘Endpoint Maintenance Ticket’ can be retrieved. If left empty, you must copy this ticket manually to the required directory (normally c:\Program Files\Lumension Security\Ticket) before you can add/modify/delete any client’s component (including directories and registry keys). See [“Uninstalling the Sanctuary Client”](#) on page 79 and your corresponding *User’s Guide* for more information.



**Warning:** If the clients are installed while the Sanctuary Application Server(s) is unavailable, they will not be able to obtain the permissions — unless they are included with policies.dat — and access to the applications/devices is refused.

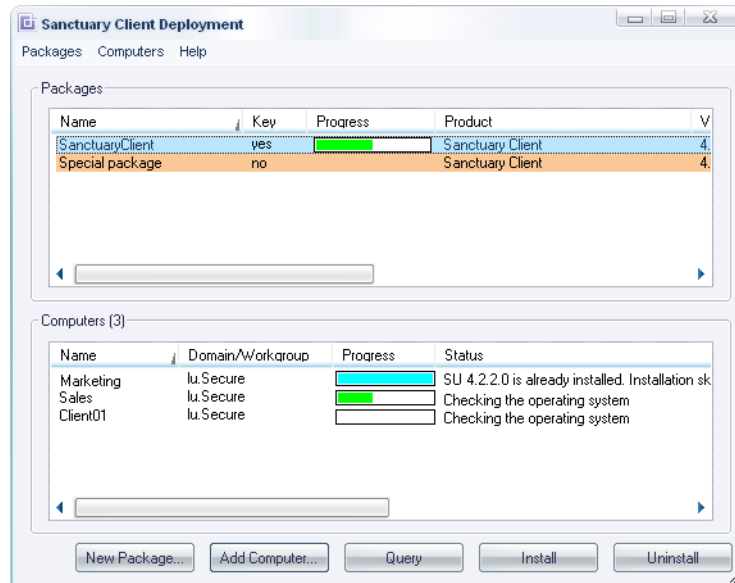


**Note:** By default client computers are not rebooted at the end of the client installation to avoid interference with the users. However, the client installation requires a reboot – even though the client is installed, it only delivers complete functionality after a reboot. The client un-installation also requires a reboot – the client remains active until the computer is rebooted.



**Note:** If the endpoint maintenance ticket cannot be retrieved from a server, you must copy it manually to each machine. You cannot modify/change/delete the client components (including directories and registry keys) if this maintenance ticket is not present (unless you deactivate the ‘client hardening’ options, see your corresponding User’s Guide for more information). The client is installed using the ‘Disabled’ option for ‘Client hardening’.

10. Click on OK. The Sanctuary *Client Deployment* Tool dialog is displayed indicating the progress of each client installation.



**Figure 8.24** Sanctuary Client Deployment Tool: Installation progress



During deployment, the dialog displays the status for each computer. The progress of the deployment is shown on the status bar, and the color of the progress bar indicates different conditions of the task, as explained in the following table:

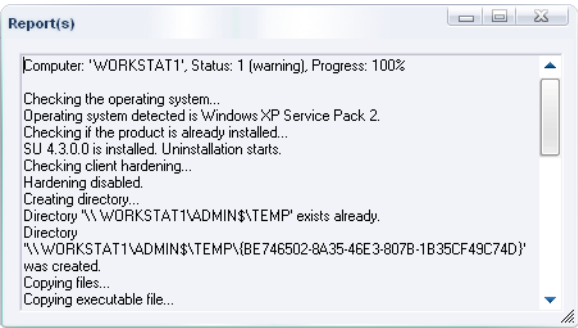
**Table 8.1** Task progress color code

Color		Description
Turquoise		Task completed successfully
Green		Task in progress with no warning
Yellow		Task in progress or completed with warnings
Red		Task in progress or stopped with an error

The status column gives you information about the deployment progress for every machine. It reports the error or the warning message when the deployment did not succeed. If the error message reported does not allow you to find the cause of the problem (unknown error, hexadecimal error code — often 0x00000643), highlight the computer in the list and select *Open Last Log* from the *Computers* menu — or from the context menu. The MSI verbose setup log file displayed should contain information about why the setup was aborted and rolled back. You can contact Lumension’s Technical Support Department for further help in analyzing the log file.

The dialog also displays a progress bar for the package being deployed. This progress bar has a mix of green, turquoise, yellow, and red indicating the clients at the various stages of deployment. The progress bar color changes to Turquoise when all tasks are completed successfully. The dialog eventually has all progress bars filled with diverse colors depending on the result of the different tasks.

You can also right click on the machine name and use the PROGRESS menu item to view information about the progress of the deployment:



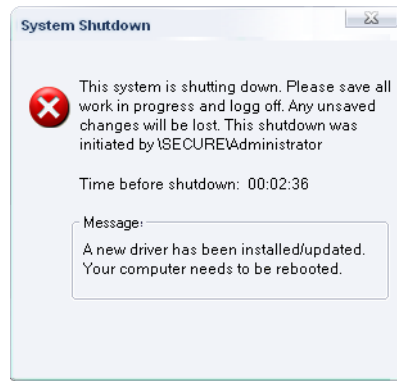
**Figure 8.25** Sanctuary Client Deployment Tool: Installation progress dialog



Here are some common mistakes to avoid:

- Trying to deploy a client package with an `sx-public.key` file that does not correspond to the key on the Sanctuary Application Server (Unspecified error).
- Trying to deploy a package while the Sanctuary Application Server is offline or cannot be contacted (firewall, wrong IP address) or/and you did not export permissions in *policies.dat* (except when you are trying to do a 'Serverless' installation).
- Trying to deploy a package on a machine where the client has just been removed and the machine has not been rebooted since. You must reboot the client machines after uninstalling.

When the deployment to a client computer is complete, it displays a *System Shutdown* dialog if configured, as shown below. The message displayed is the one you typed on the *Install/Uninstall/Reboot Options* dialog.



**Figure 8.26** Sanctuary Client Deployment Tool: Shutdown dialog in client computers

---

## Using the Command Line to Install Clients

---

If you already own a software deployment tool that you want to use instead of using our visual interface, follow these steps:

1. Create a Deployment package.
2. Copy the whole Deployment package folder to a local directory on the server (referred to as
3. 'Deploy') from which the client is to be deployed. This directory should include the msi installation file and the public key file (`sx-public.key`).
4. Install the Sanctuary Client on a list of computers by using your chosen software deployment tool to run this command-line:



```
Msiexec /i "SanctuaryClient.msi" /qn  
TRANSFORMS="SanctuaryClient.mst" /L*v %TMP%\setupcltsu.log
```



**Note:** The command above should be typed all in one line.



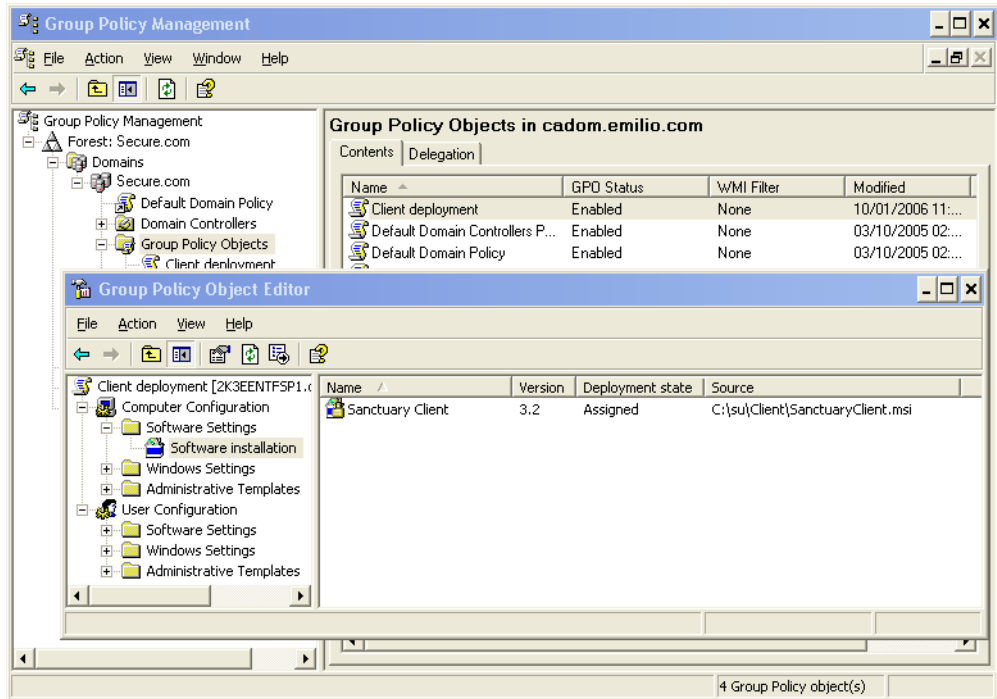
**Note:** Replace `SanctuaryClient.msi` with `SanctuaryClient64.msi` in the above line for 64-bit installations.

## Using Windows Group Policy to Install Clients

---

You can implement a computer based Group Policy for all computers in the `secure.com` domain. Group Policies can be applied to Site, Domains, or Organizational Units, depending your requirements, and the types of computers they contain.

The following example is used for demonstration purposes only and its application (domain or Organizational Unit or site) differs according to individual requirements. The *Group Policy Management Console* (GPMC) has superseded the *Active Directory Users and Computers* dialog for Windows XP (see following image).



**Figure 8.27** Using the Group Policy Management Console to install Sanctuary Client



**Note:** As with all major changes to Group Policy, it is recommended that any new Policy or changes to existing ones are tested on a development Organizational Unit first before implementing in a production environment.



**Note:** You should define the group policy package with the 'Run logon script synchronously' option activated. This will force a reboot. Beware that the client installation requires an extra reboot.

1. Create a Deployment package.



- 2. Copy the whole Deployment package folder to a local directory on the server (referred to as 'Deploy') from which the client is to be deployed. This directory should normally contain at least one file with the msi extension, one file with the mst extension, one sx-public.key file, one or several files with a cab extension and some other files.
- 3. Select *Programs* → *Administrative Tools* menu to display the *Active Directory Users and Computers* dialog.

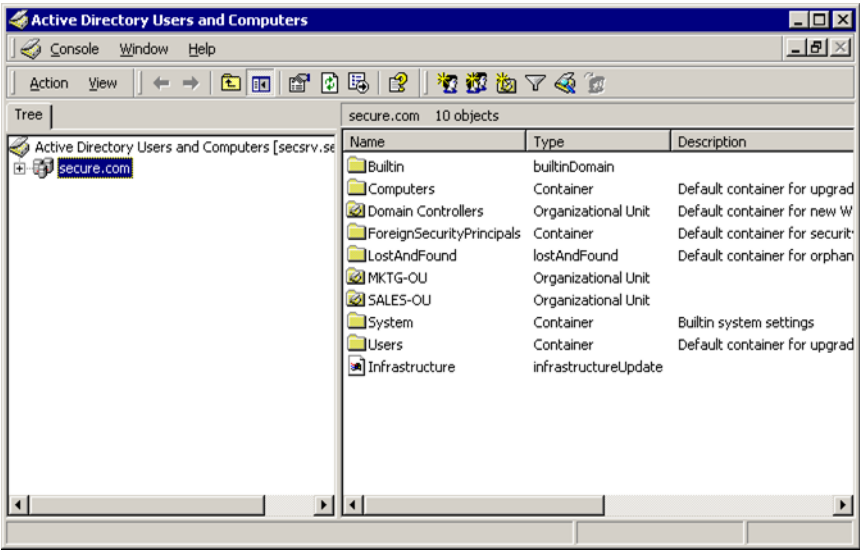


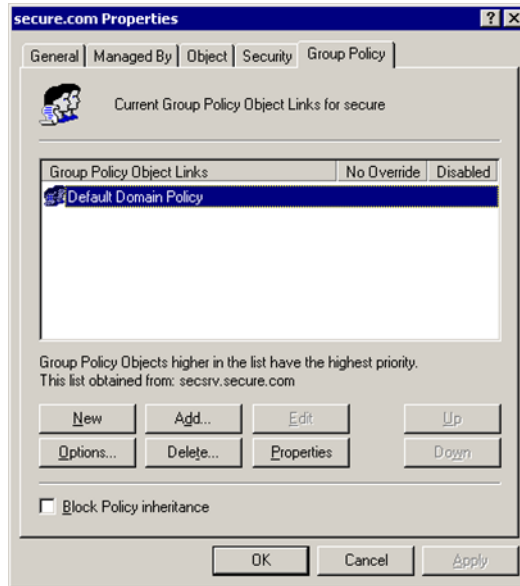
Figure 8.28 Deployment package using group policies: Select active directory

- 4. Right-click on the Domain (or Organizational Unit) and select *Properties*.





5. Select the GROUP POLICY tab.



**Figure 8.29** Deployment package using group policies: Select group policy

6. Click on NEW to create a new Group Policy, and click on EDIT.



- 7. Expand the *Software Settings* folder.

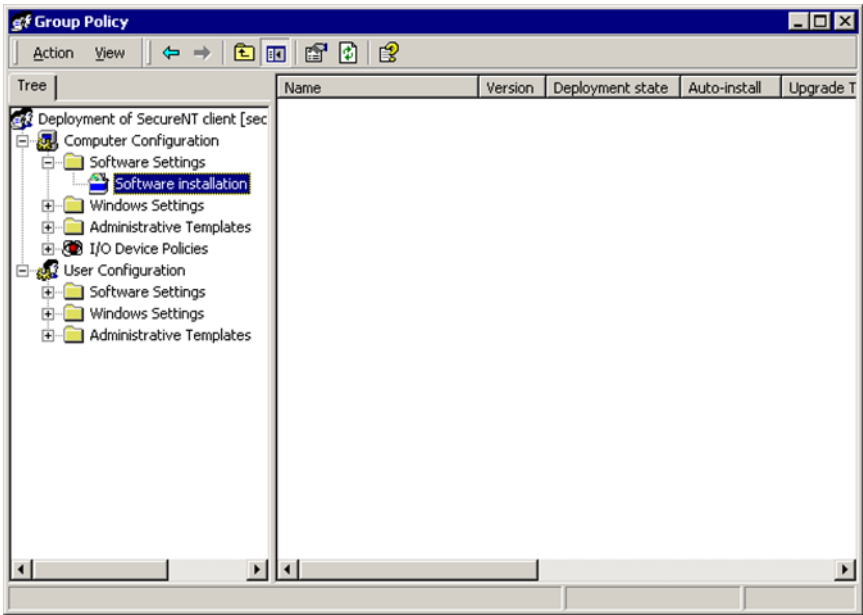


Figure 8.30 Deployment package using group policies: Software installation

- 8. Right-click on SOFTWARE INSTALLATION and select *New* → *Package*.
- 9. Browse to Deploy, select *Sanctuary Client.msi*, and click on OPEN.
- 10. In the *Deploy Software* dialog box, select *Advanced published or assigned* and click on OK.

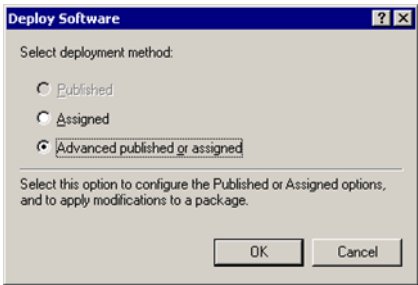
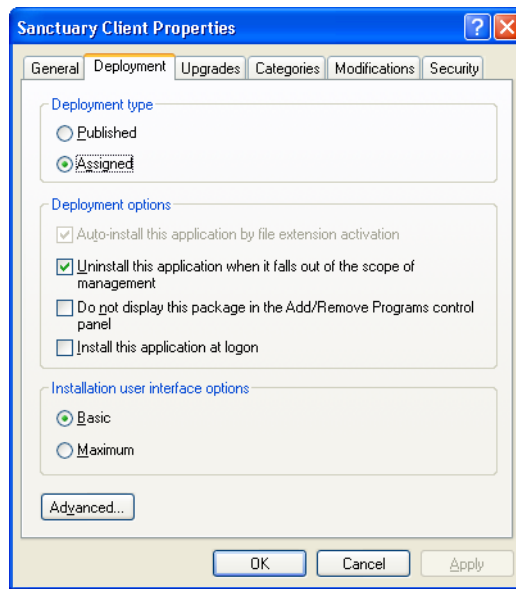


Figure 8.31 Deployment package using group policies: Deployment type



11. Accept the default name of 'Sanctuary Client', click on the *Deployment* tab and ensure that *Assigned* is selected.



**Figure 8.32** Deployment package using group policies: Deployment options

12. Display the Modifications tab and click on Add.
13. Browse to Deploy\Sanctuary Client.mst.
14. Click on Open.
15. Click on OK.

A new computer-based policy, that installs the Sanctuary Client with the configuration settings chosen as described above, is installed for all computers at boot up time (prior to client logon). A reboot is required after installation before the software becomes fully effective.



## Querying the Client Status

Once you have installed the Sanctuary Client on some client computers, it is necessary to keep track of where and which packages are installed.

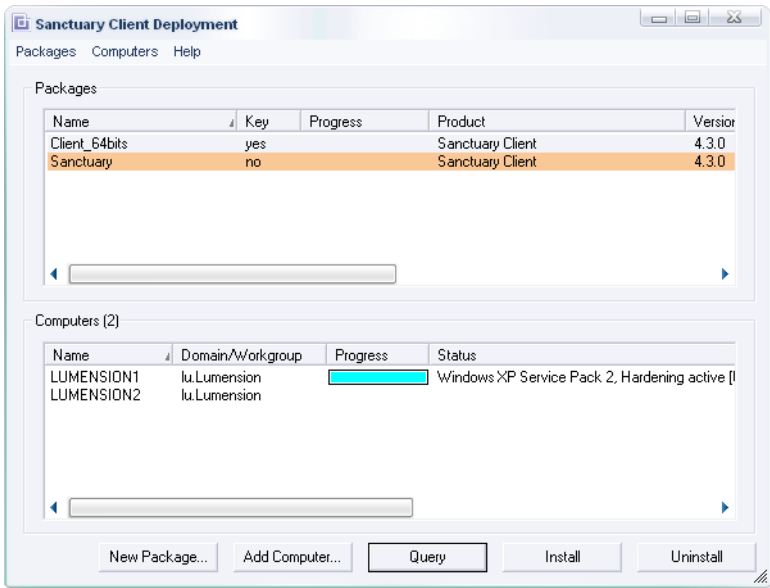


Figure 8.33 Manage deploy: Query

When you click on the QUERY button, the Sanctuary Client Deployment Tool Tool reports which version of the MSI package is installed on each computer selected in the list. It also checks if all clients are still in place and running and reports the client operating system and version, if it is using TLS protocol or not, client hardening status, etc.



**Note:** This allows you to detect, for instance, whether or not a user has the client installed on their machine but has disabled the drivers.

## Sanctuary Client Deployment Tool Menus

### Packages Menu

The *Packages* menu has the following items:



- **New**  
Allows the user to create a new deployment package, using the process in [“To Install Packages”](#) on page 97.
- **Delete**  
Deletes the selected deployment package.
- **Rename**  
Renames the selected deployment package.
- **Import public key**  
Allows the user to choose a public key to be included in the selected deployment package. The dialog shown in [Figure 8.34](#) is displayed, allowing you to select the public key to be added.
- **Set Licenses**  
Opens a dialog where you can import a license to include in the package when it is installed in *Serverless mode*. This is done so that the correct options are installed with the client.
- **Set Policies**  
Opens a dialog where you can specify a server from where to retrieve the policies. Policies are exported from this server and placed in a special file — policies.dat. This file is included in the package. See [Figure 8.35](#).
- **Test Connection**  
Allows you to verify that the Sanctuary Application Server, defined in the package, are up and running before proceeding to the deployment on the client computers. It is not available if you choose the *Serverless Mode* option.
- **Install**  
Installs the selected package on all computers in the list. (This performs the same function as the INSTALL button as described in step 7 of [“Using the Sanctuary Client Deployment Tool to Install the Sanctuary Client”](#) on page 106).
- **Uninstall**  
Uninstalls the selected package from all machines in the list.
- **Open last report**  
Displays a report describing the last install or uninstall, indicating which machines were modified and status (e.g. whether the install was successful or not).
- **Options**



Allows you to change the root directory where the packages and the Sanctuary Application Server are stored.

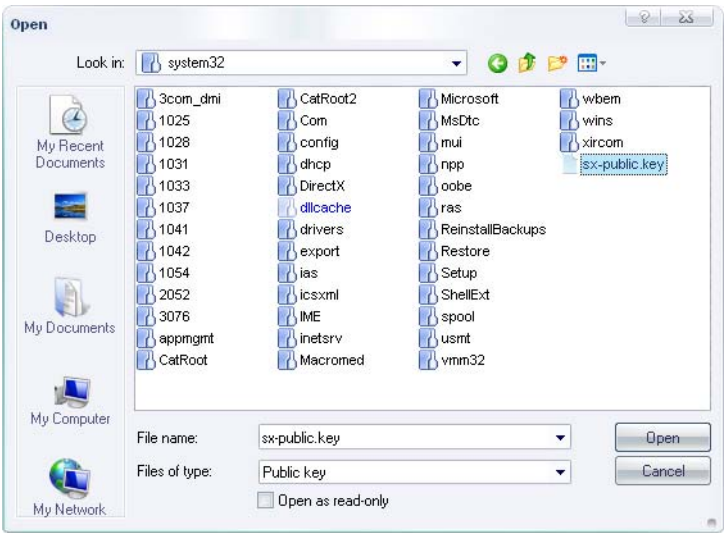


Figure 8.34 Sanctuary Client Deployment Tool menus: Import public key



Figure 8.35 Sanctuary Client Deployment Tool menus: Set policies

## Computers Menu

The *Computers* menu has the following items.

- Add  
Displays a dialog allowing you to add one or more computers to the list of computers. This is the same dialog as appears when you click on the ADD COMPUTER button.
- Remove



Removes the selected computer from the list.

- Import

Allows you to import a list of computers from an external ASCII or Unicode text file. The file must be a flat text file with one machine per line. The machine name is optionally followed by the domain name and separated from it only by a '|' sign. Every line looks like this: 'ComputerName|DomainName'.

- Export

Allows you to export a list of computers selected in the computer list to a text file. The file produced is a flat text file with one machine per line. The machine name is followed by the domain name and separated from it only by a '|' sign. Every line looks like this: 'ComputerName|DomainName'.

- Change TLS mode

When using this menu item, you can control some options governing client installation. See the description of [Figure 8.17](#).

- Reboot

Forces a reboot of the selected computers in the list of computers. You can also select here the server from where the 'Endpoint Maintenance Ticket' will be retrieved.

- Query

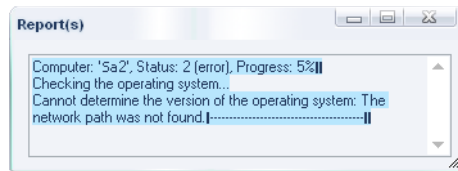
Performs the same function as clicking on QUERY (see "[Querying the Client Status](#)" on page 124). The program queries the client versions and drivers status for every machine in the list. It also reports the operating system version and service pack.

- Progress details

Displays an additional window providing details of the install / uninstall / query operation on the selected computers. An example of the progress window is shown in [Figure 8.36](#).

- Open last log

Opens the log of the last installation. An example log file is shown in [Figure 8.37](#).



**Figure 8.36** Sanctuary Client Deployment Tool menus: Progress detail



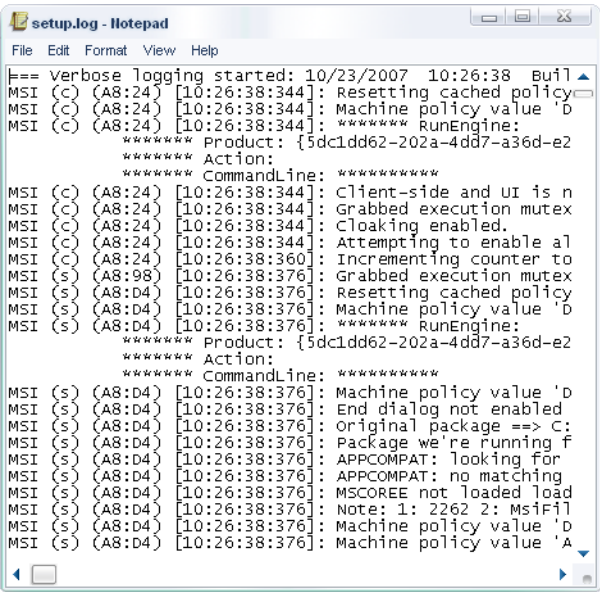


Figure 8.37 Sanctuary Client Deployment Tool menus: Log example

Help Menu

The *Help* menu has the following items.

- Help  
Displays the online help.
- About Deploy...  
Displays a dialog giving copyright and version information about the Sanctuary Client Deployment Tool

Context Menus

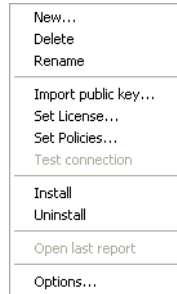
You have two context menus displayed, depending on which panel you right click:

- In the *Packages* panel the available options are those of the *Packages* menu.

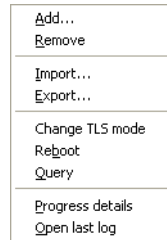




- In the *Computers* panel the available options are those found in the *Computers* menu.



**Figure 8.38** Package panel context menu

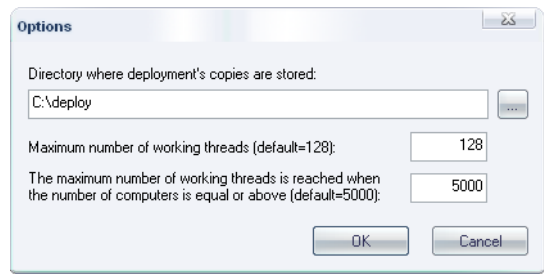


**Figure 8.39** Computers panel context menu



## The Options Screen

If you select the *Options* item in the *Packages* menu, the following dialog appears, allowing you to modify the Sanctuary Client Deployment Tool options.



**Figure 8.40** Sanctuary Client Deployment Tool menus: Options screen

The first field lets you choose the folder where you would like to store all the deployment packages.



**Warning:** Do not specify the root directory of the system drive or any other directory where existing files reside or might be created by other applications.



**Note:** If the deployment tool is installed on different machines, you might want to specify a shared directory where all instances of the deployment tool can access the company packages.

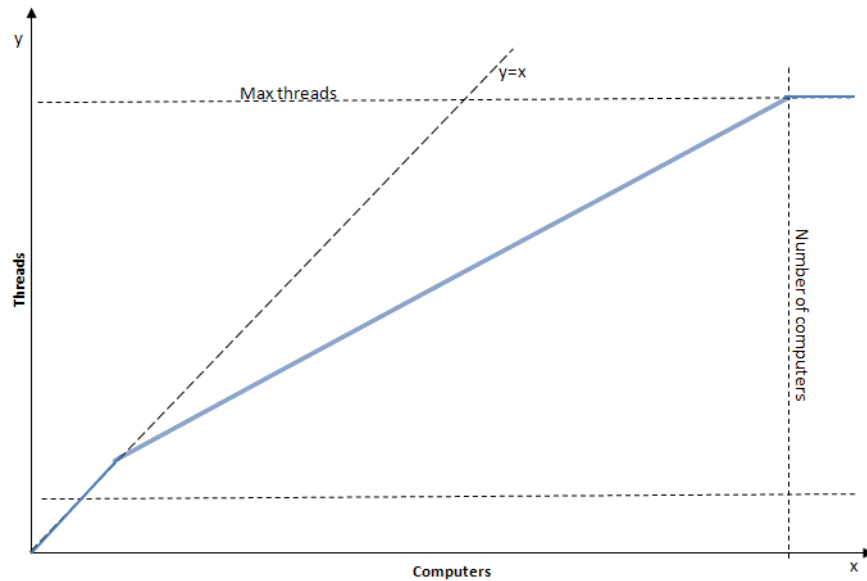
The value of the maximum number of working threads defines the highest number of deployment tasks that the program can perform in parallel. Choosing a lower value reduces the impact on the computer and network performance. Choosing a higher value allows faster deployments — if there are enough computer and network resources available.

The maximum number of working threads (simultaneous requests) specifies the number of simultaneous transactions that the tool can handle. The default value is 128. Changes to this value can be used to throttle the installation, minimizing latencies for the transactions that are performed. Reaching the maximum number of configured threads is not necessarily undesirable but means that the tool needed this many threads at peak load, but as long as it is able to serve them in a timely manner, it is adequately tuned. However, at this point connections may queue potentially overflowing when making big size installations. If you monitor your server's performance regularly and notice that its lagging, you may consider increasing the thread limits.



The third parameter defines the number of computers threshold for which the maximum number of threads will be used. This parameter specifies how the threads (previous parameter) are divided among the possible computer installations. To compute the number of simultaneous requests, the tool counts the number of active requests, adding one to the number when a new request arrives or subtracting one when it finishes the request. The tool checks to see if it is already processing the maximum number of requests. If it has reached the limit, it defers processing new requests until the number of active requests drops below the maximum amount.

Both parameters are combined to allow you to fine-tune the application performances. The relation that links both parameters is explained in the following figure.



**Figure 8.41** Sanctuary Client Deployment Tool menus: Number of threads vs. number of computers





## 9 Using the SXDomain Command Line Tool

This chapter explains how you can synchronize domain information with that contained in the Sanctuary Database. The information in this chapter is relevant to all Sanctuary products.

### Introduction

The SXDomain command-line tool is an alternative to the Add Domain / Synchronize Domain items in the *Tools* menu on the Sanctuary Management Console. You can use it to:

- Add new domains to the list of those managed by Sanctuary
- Add and update information about users, groups and computers in a domain already managed by Sanctuary
- Add/synchronize local users and groups
- Add/synchronize computers that are part of a workgroup

*SXDomain.exe* can be found within the C:\Program Files\Lumension Security\Sanctuary\SXTools directory (assuming that you installed the Sanctuary software under C:\Program Files\). Use the command prompt to run the file from this directory.

### The SXDomain Parameters

The SXDomain command line should be entered as follows:

```
SXDomain [-s servername] domain1 [domain2 ...]
```

The parameters in this command line are defined below:

- **-s servername**  
The fully qualified domain name or IP address of the computer on which Sanctuary Application Server is running.
- **-i**  
Instructs the utility to read domain names to add or synchronize from a standard input stream (interactive mode).
- **-e**  
Instructs the utility to write the domain names that could be neither added nor synchronized to a standard error stream.
- **-u username**  
The user name used to authenticate on the remote computer. Do not include the domain prefix, only the user name.
- **-p password**  
Password. SXDomain prompts you for one, if not supplied.

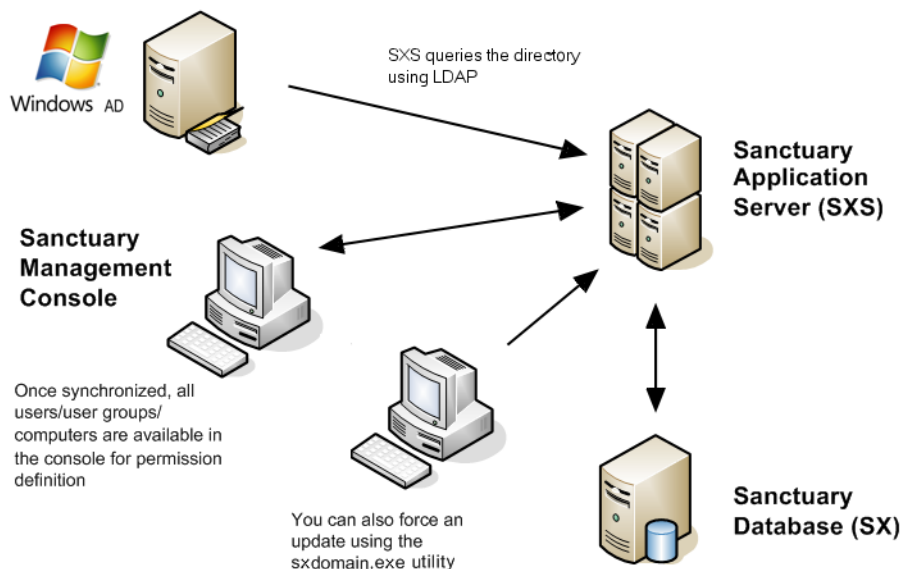


- -q

Do not prompt for the user's name or password if they cannot be authenticated.

- domain

The name of the domain(s), computer(s), or IP address that you want to add or refresh. If you do not use the -i parameter, you must at least specify a list of domains to work with.



**Figure 9.1** Active Directory objects' synchronization

## Examples

For the following examples:

- SXS\_SERVER is the name of the computer running Sanctuary Application Server.
- CLIENT is the name of the computer running Sanctuary Client.

To refresh the domain information for the domain DOMAIN, use the following command.

```
SXDOMAIN -s SXS_SERVER DOMAIN
```

To refresh details of the local users of the computer CLIENT (which can be a domain controller in case it does not show up after its domain was added):

```
SXDOMAIN -s SXS_SERVER CLIENT
```

To refresh details of the local users of the computer `CLIENT`, where `CLIENT` is part of a workgroup rather than a domain. The username and password of the computer's local administrator should be used in the following command:

```
SXDOMAIN -s SXS_SERVER -u username -p password CLIENT
```



**Warning:** Windows XP has by default the 'Simple file sharing' option set. This option essentially turns the computer into 'anonymous access only', preventing Sanctuary Application Server from retrieving its local users. If it is set, turn it off using the Tools → Options dialog of the Windows Explorer.

To synchronize a number of domains, you can enter the names into a text file (one name per line of text) and supply it as input to the utility as shown below.

```
SXDOMAIN -s SXS_SERVER -i < mydomains.txt
```

You can also redirect the names of any domain that failed to synchronize to a file by means of the standard error stream:

```
SXDOMAIN -s SXS_SERVER -i -e < mydomains.txt > error_list.txt
```

If you prefer, you can synchronize domains interactively:

```
SXDOMAIN -i
```

Type in the name of each domain followed by the ENTER key. Once you are finished, use Ctrl+C to end the interactive mode and exit to the operating system.

## Scheduling Domain Synchronizations

---

You can schedule domain synchronizations with your favorite task scheduler. Here is a procedure using the Windows Task Scheduler.

In the `C:\Program Files\Lumension Security\Sanctuary\SXTools` directory, you should create a batch file `sxsynch.bat` containing the following line:

```
CMD /C SXDOMAIN -s SXS_SERVER -i -e < mydomains.txt >
error_list.txt
```

The `mydomains.txt` file holds the names of the domains to synchronize (one name per line of text). The list of domains that failed to synchronize is redirected to the `error_list.txt` file.



1. Go to the *Control Panel*, choose *Scheduled Tasks* and then *Add Scheduled Tasks*. The following screen is displayed.

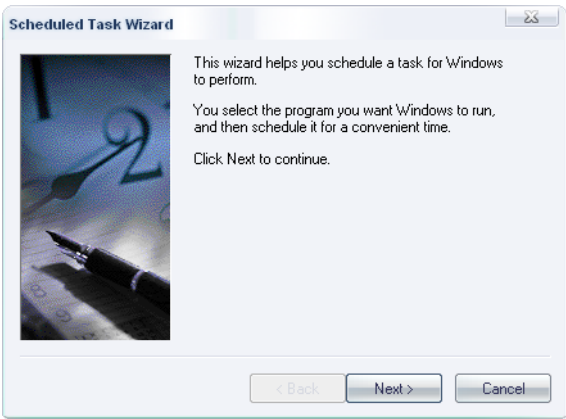


Figure 9.2 Scheduled task: First step

2. Click on *Next*.
3. In the following screen, click on *Browse* and select the *sxsync.bat* file:

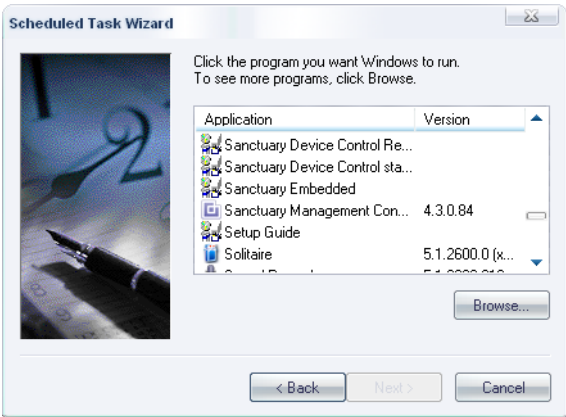


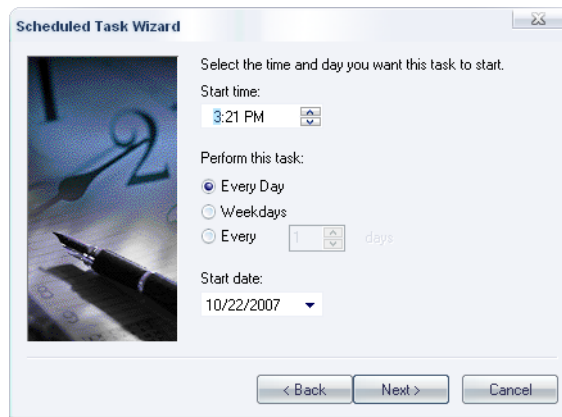
Figure 9.3 Scheduled task: Select program



4. In the next two screens, choose how often you want the task to be performed:



**Figure 9.4** Scheduled task: Select period (1/2)



**Figure 9.5** Scheduled task: Select period (2/2)



- 5. Specify an account that has rights to use the Sanctuary Management Console. This is the account that runs the sxdomain command:



Figure 9.6 Scheduled task: Select account

- 6. Click on FINISH to end the Wizard:



Figure 9.7 Scheduled task: Ending the wizard



**Warning:** It is important to synchronize domains in order to have ‘fresh’ information available. If you do not do this in a regular basis, you could have bad surprises when some users, machines, or domains do not appear in your database.



**Warning:** SQL activity may increase substantially when large domains are synchronized.



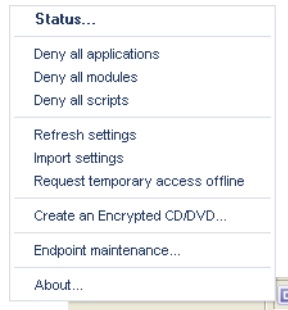


# 10 Registering your Sanctuary Product

This chapter explains what happens when you register your Sanctuary product. It provides examples of information contained in a typical license file. The information in this chapter is relevant to all Sanctuary products.

## Licensing

Each Sanctuary Application Server has a license file that specifies whether you have a valid copy of one or several of our Sanctuary programs: Sanctuary Application Control Server Edition, Sanctuary Device Control, etc. Depending on the type of license, your client computers either show or do not show the options appropriate to each one of the installed programs. The following image was taken in a network that has Sanctuary Device Control and Sanctuary Application Control installed.



**Figure 10.1** Client's options when several Sanctuary products are installed

If the license information changes, for example when a new Sanctuary product is added, the client is informed and its options changes accordingly.

## Obtaining a License

### Evaluation License

You can obtain an evaluation license by registering on Lumension's website ([www.lumension.com](http://www.lumension.com)). From there, select the product page for the Sanctuary product you want, and then select *Evaluation Request*. Fill out the Evaluation License Request form. Once your request is approved, you will receive a copy of the license file – save it into the %SYSTEMROOT%\SYSTEM32 directory.

An evaluation license provides you with the full functionality of Sanctuary software, but with the following limitations:



- It only lasts one month.
- No more than 10 Sanctuary Application Servers can be installed in parallel.
- No more than 100 client computers can be administered.

### Full License

When you purchase one of our Sanctuary products, a new license key is sent to you by e-mail. This license key is specifically configured for the license you have purchased. You do not need to uninstall the software when switching from an evaluation license to a full license. The Sanctuary Application Server uses the new license file within an hour. If you want Sanctuary Application Server to use the new license file immediately, restart the Sanctuary Application Server service on every Sanctuary Application Server machine where the new license file was copied.

### License File Location

---

When you receive the license file, copy it to the %SYSTEMROOT%\SYSTEM32 folder of each computer that runs Sanctuary Application Server. It is *not* required to be present on client machines.



**Warning:** If you are using more than one Sanctuary Application Server, the same license file must be used on all the servers.

### License File Format

---

A Sanctuary license file comprises a series of name and value pairs, one per line. It includes the following important information:

- **ProjectName**  
Identifies the software product for which the license is valid.
- **ExpiryDate**  
Validity of the license file.
- **LicensedClients**  
Number of clients that can be registered in the Sanctuary Database. This corresponds to the sum of the number of computers where Sanctuary Client is used.
- **LicensedSessions**  
This limits the number of sessions that Sanctuary Application Server allows. Exceeding this limit only causes warnings to be displayed. A session, in this context, refers to a 'logon session'. Such a logon session is created for every interactive logon of a user on a Sanctuary protected computer. Logon sessions are also created for services that run under a 'real' user account (as opposed to LocalSystem), and under certain circumstances by some server programs (mail, web, FTP servers, and so on).

- **LicensedServers**  
Number of instances of Sanctuary Application Server that may be run at the same time. Sanctuary Application Server refuses to start if it detects a number of already running Sanctuary Application Server instances exceeding this limit.
- **ProductName**  
The full name of the product for which the license was created.
- **ClientName**  
The name of the customer to whom the product was licensed.
- **GeneratedOn**  
The date on which the license was created. This is useful if you are unsure when to renew your maintenance contract.
- **Serial#**  
The serial number of this license.
- **LicensedTo**  
The name and/or email address of the person to whom the license was issued.
- **LicensedCPUs**  
Number of CPUs for which this license was created.
- **IPAddress**  
The IP address assigned to the Sanctuary Application Server.



**Warning:** The Sanctuary Application Server refuses to start if you modify the license file – even just changing or adding a comment or blank line.

Every computer protected by Sanctuary Client registers itself in the online table of the Sanctuary Application Server during the boot sequence of the client. Counting these entries gives the number of 'clients'. This licensing mode is ideal for corporate environments where there is essentially one user per computer.

In ASP and Terminal Services environments, one computer may support hundreds of users. In these situations, the license is expressed in terms of 'sessions', a session being created when a user logs on and removed when a user logs off. Inaccuracies are created by services (programs that run unattended in the background), if the administrator has configured them to run with the identity of a regular user instead of LocalSystem, and by server software that verifies the identity of its users by simulating a logon. An example would be IIS with password-protected pages. In addition to that, users may create additional sessions using secondary logon services ('runas' command in Windows 2000/XP/2003/Vista).

In either case, Lumension adjusts the actual license limits to account for these requirements.



### License-Related Sanctuary Application Server Actions at Start-Up

---

On start up, Sanctuary Application Server immediately verifies the license file. If any of the following conditions is true, Sanctuary Application Server quits directly:

- The license is invalid (has been tampered with or is missing).
- The project name is invalid.
- The product expiry date has ended.
- The number of licensed servers has been exceeded.

No other license related conditions cause Sanctuary Application Server to refuse to start.

### License-Related Sanctuary Application Server Actions While Running

---

Once every hour, or thereabouts, Sanctuary Application Server verifies the license file. This means that an upgrade to a license is done by simply copying the new license file over the old one.

Sanctuary Application Server terminates if the license file is missing, has been tampered with, the project name is invalid, or the expiry date is exceeded.

If any of the following license-related conditions are true, Sanctuary Application Server logs a message when running interactively:

- The expiry date has ended.
- The *LicensedCPUs* value is less than the number of processors installed in the computer.
- The *IPAddress* key does not list at least one IP address belonging to the computer.
- The *LicensedClients* value has been exceeded.
- The *LicensedSessions* value has been exceeded.
- The *LicensedServers* value has been exceeded.

### License-Related Client Actions

---

The client applies licensed Sanctuary policies immediately even if they have not been correctly configured or defined. For example, if no proper application permissions have been set in Sanctuary Application Control Server Edition, the client blocks all attempts to execute programs in the machine, even the logging program, with fatal consequences. Not configuring device permissions for Sanctuary Device Control applies the most restrictive policy, no access to external devices.

An upgrade may surprise your clients when you install a license for several products but only one is active. The client shows 'unused' options.





Likewise, the client ceases to apply Sanctuary policies if not licensed. This only affects customers violating the license, but this can also be a result of incorrect license management and can represent a security risk for your organization.





# A Detailed System Requirements and Limitations

The information in this appendix applies to all Sanctuary software suite products unless otherwise specified.

This appendix specifies the minimum system requirements for the different components used in a Sanctuary implementation and details the limitations of installing the Sanctuary Client on Terminal Servers and Citrix environments for some products of our suite.

## System Requirements

**Table A.1** Sanctuary Application Server system requirements

Operating System	Disk space	Memory	Other
<ul style="list-style-type: none"><li>• Microsoft® Windows® 2000 Server (SP4 or later)</li><li>• Windows Server 2003 (SP1 or later)</li></ul>	<ul style="list-style-type: none"><li>• 4 MB free disk space for program files</li><li>• 15 MB for the installation</li></ul> <p>(Using an NTFS disk partition)</p>	256 MB (512 MB recommended)	<ul style="list-style-type: none"><li>• MDAC v2.6 SP1 or later if you are using Windows 2000 Server</li><li>• A Certificate Authority installed and configured if TLS protocol is chosen for intra Sanctuary Application Server communication</li></ul>
All operating systems are 32-bit unless noted otherwise			



**Table A.2** Sanctuary Database system requirements

Operating System	Disk space	Memory	Others
<ul style="list-style-type: none"> <li>Microsoft® Windows® 2000 Server (SP 4 or later)</li> <li>Windows 2000 Professional</li> <li>Windows XP Professional (SP2 or later)</li> <li>Windows Server 2003 SP1 or later</li> <li>Windows Vista SP0 or later</li> </ul>	<ul style="list-style-type: none"> <li>1 MB free disk space for program files</li> <li>40 MB for the installation</li> <li>From 10 Mb up to several GB for data (depending on the number of users)</li> </ul> <p>(Using an NTFS disk partition)</p>	512 Mb (2 GB recommended)	<ul style="list-style-type: none"> <li>Microsoft SQL Server 2000 SP4</li> <li>Microsoft SQL 2005 SP2 or later</li> <li>Microsoft SQL 2005 64-bit SP2 or later</li> <li>SQL Server 2005 Express Edition (requires Microsoft .NET Framework 2.0)</li> <li>MDAC V2.6 SP1 if using Windows 2000</li> </ul>
All operating systems are 32-bit unless noted otherwise			

**Table A.3** Sanctuary Administration Tools system requirements

Operating System	Disk space	Memory	Display
<ul style="list-style-type: none"> <li>Microsoft® Windows® 2000 Server (SP4 or later)</li> <li>Windows 2000 Professional</li> <li>Windows XP Professional (SP2 or later)</li> <li>Windows Server 2003 (SP1 or later)</li> <li>Windows Vista**</li> </ul>	<ul style="list-style-type: none"> <li>150 MB free disk space for program files</li> <li>15 MB for the installation</li> </ul> <p>(Using an NTFS disk partition)</p>	256 MB (512 MB recommended)	1024x768
All operating systems are 32-bit unless noted otherwise			
**Consult us before installing the Sanctuary Management Console in this system			



**Table A.4** Sanctuary Client system requirements

Operating System			Disk space	Memory	Others
Sanctuary Device Control or Sanctuary Application Control	Sanctuary Embedded Devices	Sanctuary Application Control Server Edition or Sanctuary Application Control Terminal Services Edition			
<ul style="list-style-type: none"> <li>• Microsoft® Windows® 2000 Professional (SP 4 or later)</li> <li>• Windows XP Professional (SP2 or later) 32 &amp; 64-bit</li> <li>• Windows XP Tablet PC Edition SP2</li> <li>• Windows Vista SP0 or later (32 &amp; 64-bit)</li> <li>• Windows 2003 SP1 or later (32 &amp; 64-bit)</li> </ul>	<ul style="list-style-type: none"> <li>• Microsoft Windows Embedded for Point of Service (WEPOS)</li> <li>• Windows XPe (SP2 or later)</li> </ul>	<ul style="list-style-type: none"> <li>• Microsoft Windows 2000 Server (SP4 or later)</li> <li>• Windows Server 2003 (SP1 or later)</li> </ul>	<ul style="list-style-type: none"> <li>• 8 MB free disk space for program files</li> <li>• 15 MB for the installation</li> <li>• With Shadowing enabled (when using Sanctuary Device Control), disk space requirements can grow up to several GB</li> </ul> <p>(Using an NTFS disk partition)</p>	256 MB (512 MB recommended)	<ul style="list-style-type: none"> <li>• Novell client v4.91 SP1 or later if connected to a Novell environment.</li> <li>• A Certificate Authority installed and configured if TLS protocol is chosen for Client-Sanctuary Application Server communication.</li> </ul>
All operating systems are 32-bit unless noted otherwise					



Table A.5 Sanctuary common requirements

If using central encryption or TLS communication protocol	If using Novell
<ul style="list-style-type: none"><li>• A valid Certificate Authority installed to issue and manage certificates if you want encrypted client Sanctuary Application Server and intra-Sanctuary Application Server TLS communications. This authority is also needed if you plan to centrally encrypt removable devices (if using Sanctuary Device Control).</li><li>• If no Certificate Authority is found, you can still encrypt devices (with some limitations) and the communication channel is assured by signing messages with a private key.</li></ul>	<p>On the computer used to synchronize Novell's objects (we recommend installing all these components on the same machine as the one used to host the database):</p> <ul style="list-style-type: none"><li>• Novell (and optionally ZENworks) client v4.91 SP1 or later</li><li>• NDAP (for workstation object synchronization)</li><li>• The synchronization script</li><li>• Access to Sanctuary's database.</li></ul> <p><b>Notes:</b></p> <ul style="list-style-type: none"><li>• Synchronizing environments running versions of NetWare earlier than 6.5 is not supported.</li></ul>



**Note:** You can find the NDAP components required for Novell synchronization on the installation CD or on Novell's Web site.



**Warning:** You should resolve all hardware conflicts before installing Sanctuary solutions. You can use Windows' Device Manager to troubleshoot and fix software-configurable devices. All hardware devices that use jumper pins or dip switches must be configured manually.



**Note:** If you plan to use encrypted devices, when installing Sanctuary Device Control, you will need Active Directory and DNS installed and properly configured. The Microsoft Certificate Authority must be installed, properly configured, and published. You will also need this Certificate Authority when using encrypted communications between Sanctuary Application Servers (SXS) or SXS-Sanctuary Client Driver.



**Warning:** For the Sanctuary Database installation, we strongly recommend that you install the latest Service Packs. You should not bring a database into use without installing at least SQL 2000 SP4. Otherwise, your database is not protected against the slammer worm.



**Warning:** The Sanctuary Application Server cannot be installed on Windows XP, Windows 2000 PRO, or Windows Vista.



**Warning:** Memory requirements may vary based on your system, operating system, and the software you already have installed on the platform where you will be installing Sanctuary. Large installations and some operating system will require significant extra memory, especially in those cases where the machine is already close to its memory limits. The same applies to the client installation, where more memory may be required if there is already other memory intensive software installed.

## Sanctuary Device Control

---

### Terminal Services Limitations

The Terminal Services administration mode and the remote desktop functionality allow access to computers remotely. This section details how the Sanctuary Client Driver enforces security when devices are accessed remotely.

Sanctuary Device Control normally applies the permission of the user accessing the device, be it a remote user or the user working interactively with the computer. This is the case for the device classes for which the device access is performed in the context of the user who initiated the access: BlackBerry (USB), DVD/CD (**Read access**), Com, LPT (**not** when used for printing), Palm OS Handheld Devices (USB), Removable, Tape, Unauthorized Encrypted Media, Windows CE Devices (USB).

Certain kinds of device accesses are not performed in the context of the user who initiated the access. Instead, a proxy that normally has privileged access to the system (a service or a driver) carries them out. DVD/CD **writing** is one example; there are a few other ones: modems, scanners, smart card readers, printers (either USB or connected to the LPT port) and unknown devices.

When the Sanctuary Client Driver detects such 'proxy' access, it tries to determine the identity of the user who initiated the access. This is done successfully when there is only one interactive user.



When there is one interactive user and one remote user on the same computer (i.e., when there are more than one logon sessions with different session IDs), the client cannot determine reliably the identity of the user that initiated the access. In such conditions and only for the DVD/CD burning, modems, scanners, smart card readers, printers (USB or LPT) and unknown devices classes, the Sanctuary Device Control will deny all proxy access. It means for example that the users will not be able to write DVDs/CDs when somebody accesses their machine remotely even if both the interactive user and the remote user have a Read/Write access to the DVD/CD drive. The user accessing the machine remotely will not be able to write DVDs/CDs either.

### The RunAs Command Limitations

There is a situation similar to the Terminal Services issue when using the RunAs Commands or equivalent. This type of command is often used in logon scripts.

Certain kinds of device access are not performed in the context of the user who initiated the access. Instead, a proxy that normally has privileged access to the system (a service or a driver) carries them out. DVD/CD **writing** is one example; there are a few other ones: modems, scanners, smart card readers, printers (either USB or connected to the LPT port) and unknown devices.

When the Sanctuary Client Driver detects such ‘proxy’ access, it tries to determine the identity of the user who initiated the access. This is done successfully when there is only one interactive user. The user cannot be determined when there are active RunAs logon sessions.

When the Sanctuary Client Driver detects RunAs logon sessions, and only for DVD/CD burning, modems, scanners, smart card readers, printers (USB or LPT) and unknown devices classes, the RunAs Logon sessions are mapped to the interactive logon session with the same session ID. Thus, all RunAs processes **will have exactly the same access as the interactive user who launched them**. Using the RunAs command to change the level of access to these devices is not possible.

**Example 1:** Bill has no access to DVD/CD. John has Read/Write access to DVD/CD. If Bill uses a RunAs command to run the DVD/CD burning software under the credentials of John he will **not** be able to create new CDs. Bill will have to log off and log on as John to create new DVDs/CDs. Since writing a DVD/CD requires a proxy, it is subject to the limitation described in this section.



**Note:** Writing a DVD/CD requires a proxy and is subject to the RunAs limitation, whereas reading a DVD/CD is not.

**Example 2:** Bill has no access to the Floppy. John has Read/Write access to the Floppy. If Bill uses a RunAs command to run the Windows File Explorer under the credentials of John, he will be able to read and write to the Floppy. Indeed, access to the Floppy is done without a proxy. The limitation described in this section does not apply to this device.



## B Registry Keys

The information in this appendix applies to all Sanctuary software suite products.

### Sanctuary Application Server Registry Keys

The following table contains details of each registry key entry used for Sanctuary Application Server. All Sanctuary Application Server entries are of type REG\_SZ (= string value). The entries in the following table are found within the following key:

HKLM\system\CurrentControlSet\services\sxs\parameters



**Warning:** Keys whose names are marked with an asterisk \* should not be modified except under the supervision of Lumension Support personnel.

### Database Connection Loss Registry Keys

The Sanctuary Application Server continues to run even if it has an intermittent database connection. It ignores database connection problems for a certain period of time, retrying connections to the Sanctuary Database until it succeeds. If the problems persist, the Sanctuary Application Server stops accepting client and console connections until it detects database connectivity has been restored.

You can configure the following parameters to determine the exact behavior of the Sanctuary Application Servers if they lose connection to the Sanctuary Database:

**Table B.1** Sanctuary Application Server registry keys (Database related)

Key Name	Description	Default
DbConnectionCount	The number of database connections in the connection pool.	20
DbConnectionMaxCount	The maximum number of DB connections (if it is less than DbConnectionCount, it will be assumed equal to it)	40
DbConnectionPoolTimeout	The timeout, in seconds, for connection acquisition from the DB pool. If no connection can be acquired within the timeout, an attempt to grow the pool will be made. Note that if the pool has reached the maximum number of connections, no new connections will be created and the wait will be repeated.	15



**Table B.1** Sanctuary Application Server registry keys (Database related)

Key Name	Description	Default
DbConnectionString	Driver, server, database, and either a trusted connection, or username and password. The default value is 'Provider=sqloledb;Data Source=; Initial Catalog=sx; Trusted_Connection=yes;'	See description
DbInitializationDelay*	Number of seconds that Sanctuary Application Server waits before contacting the SQL Server	300
DbLossLatency	The graceful DB loss period, in seconds, during which the server accepts client and console connections after DB loss has been detected (3600 is one hour).	3600
DbPingPeriod	The periodicity, in seconds, of DB pinging when the server has stopped accepting client and console connections (60 is one minute).	60

Log Insertion Process Registry Keys

The following table shows all registries that can be modified to fine-tune the endpoint data reception facility that controls logs and shadow files received from the Sanctuary Client. The endpoint data reception facility places all incoming data in a staging queue, from which endpoint data batches are generated and dispatched in a regular fashion, without stressing the database. Advanced configuration parameters are available to fine-tune batching and dispatching of endpoint data; statistical information is available in the Windows Application Event Log to help examine and fine-tune the configuration:

**Table B.2** Sanctuary Application Server registry keys (Log insertion process)

Key name	Description	Default
edrBatMaxDuration	Max batching time per batch, in seconds. If a batch has not reached the minimal number of entries, but exceeded this duration being batched, it will be put into the queue.	30
edrBatMinEntries	Minimum entries per batch. A batch will be put into the queue as soon as it has at least this number of entries, or it has been being batched longer than the max batch duration (see next).	10000
edrBatThreads	The number of batching threads.	2
edrDspPause	Successful dispatch mean sleep time, in seconds. Zero by default. Once a dispatcher submits a batch to the DB successfully, it will sleep that long.	0



**Table B.2** Sanctuary Application Server registry keys (Log insertion process)

Key name	Description	Default
edrDspPauseFail	Initial unsuccessful dispatch mean sleep time, in seconds.	60
edrDspRetryCount	Max number of retries for unsuccessful dispatches.	5
edrDspThreads	The number of dispatching threads.	1
edrQueLength	The length of batch queue.	3
edrStaPeriod	The periodicity of statistical output, in seconds. Zero disables statistical output (43200 is 12 hours).	43200
edrTmpTimeout	Max file slot allocation time, in seconds. When clients upload data, temporary files are allocated. The temporary directory can contain a limited number of files. If the directory becomes congested and no more temp files are available, the server will wait up to this duration for a free temp file slot.	30

## Debugging Registry Keys

The following registry keys are used to debug Sanctuary Application Server:

**Table B.3** Sanctuary Application Server registry keys (Debugging purpose)

Key name	Description	Default
Debug*	If 'yes' or '1' and if Sanctuary Application Server runs as a service, it attempts to launch a debugger and attach it to itself.	no
Log file name	Gives the name of the log file written if 'Log to file' is true.	sxs.log*
Log to console	If 'yes' or '1', sends debug messages to the console, if any.	no
Log to dbwin	If 'yes' or '1', sends debug messages to Dbwin32.	no
Log to file	If 'yes' or '1', sends debug messages to the log file (see the Log file name entry).	no*
LogMonitorDlls	Not used for Sanctuary Device Control. Key used by Spread Check. If configured, it would also monitor the spread of DLLs that have been authorized implicitly in the DLL don't care mode. If not configured, only applications and explicitly authorized DLLs are monitored. See the Sanctuary Application Control Suite User Guide for more details.	no



**Table B.3** Sanctuary Application Server registry keys (Debugging purpose)

Key name	Description	Default
LogMonitorPeriod	Not used for Sanctuary Device Control. Period, in seconds, between two checks.	300
LogMonitorResetOptions	Not used for Sanctuary Device Control. Number of distinct users that must execute the same locally authorized executable for an alert to be issued.	yes
LogMonitorThreshold	Not used for Sanctuary Device Control. Controls whether the global user option is set to blocking mode when the alert is generated, if 'no', Sanctuary Application Server only issues a message in the event log, if 'yes', it issues the same message, sets and pushes the option, and then issues another event log message informing if the set+push was successful. The purpose of this message is to notify the administrator that there was a spread check action.	10
VerboseSyncLogging	If set to 'yes', the Sanctuary Application Server will log all the important attributes of the objects that it retrieves during a domain synchronization. In order to see the results in the Sanctuary Application Server log file, the Log to file value must be set to 'yes'. If the Log to file value is already set to 'yes', you do not need to restart the Sanctuary Application Server service to take the VerboseSyncLogging Value into account. You should not set this option to 'yes' permanently for performance reasons.	no
*You should specify a R/W path accessible by the Sanctuary Application Server service account for this log file		

General Registry Keys

These registry keys are the general ones:

**Table B.4** Sanctuary Application Server registry keys (general keys)

Key name	Description	Default
AdoVersion*	A string representing the version of ADO objects to use. Default: ''. For Windows 2000, try '.2.5'. Note that the leading dot must be present, unless an empty string is given.	empty
Concurrency*	How many running threads are allowed by the IOCP. '0' (zero) means 'auto' and is equivalent to one thread per CPU. Minimum: 0, maximum: MaxThreads.	0



**Table B.4** Sanctuary Application Server registry keys (general keys)

Key name	Description	Default
DataFileDirectory	The base directory under which the Sanctuary Application Server stores data files (log files, for instance). If multiple Sanctuary Application Servers are in use, their DataFileDirectory entries may all resolve to the same directory on disk. This is the directory created during the Sanctuary Application Control setup process. All servers can optionally write to the same, shared, directory or you can opt for having different ones for each server (see <a href="#">Figure 1.1</a> , on page 2 ).	c:\datafile
OnLineMonitorPeriod	A value in minutes stating the period after which a “maintenance + clean” cycle is started. This cycle purges all offline machines from the active computer table kept by the Sanctuary Application Server. This table is used, among other things, to generate the Online Machines report. This avoids “freezing” the console while doing and update when your organizations has a large number of machines to monitor. This parameter is used in combination with the following one.	60
OnLineStateExpiry	A value in minutes defining the period in which If a client has not communicated with the Sanctuary Application Server, it its drop from its table of active ones with out further notification until another communication is stablished. This parameter is used in combination with the previous one.	180
Products	Internal use. Do not modify.	n/a

## Security Registry Keys

These registry keys are related to security configuration and parameters:

**Table B.5** Sanctuary Application Server registry keys (security registry keys)

Key name	Description	Default
CertificateQueryPeriod	(optional) Controls the periodicity the Sanctuary Application Server checks user's certificates published in AD.	180
CommVer	The Sanctuary Application Server uses this key to determine which communication protocol version it should use. '0' (zero) indicates that there are still older version of the client in use (prior to v3.1) while '1' is used when the installation only has clients v3.1 or 3.2. A value of '2' indicates a client version 4.0, and '3' is used for version 4.1 or greater when using TLS.	3 (only when using TLS)



**Table B.5** Sanctuary Application Server registry keys (security registry keys)

Key name	Description	Default
MaxSockets*	The maximum number of TCP connections that are allowed at any one time. The length of the listen queue backlog imposes an additional constraint. This queue holds connection requests that cannot be accepted because Sanctuary Application Server is momentarily busy or because it has reached the limit imposed by MaxSockets. Sanctuary Application Server always sets the length of the listen queue backlog to the maximum (5 on Home/Professional editions of Windows, 200 or more on the Server editions). Note that this entry does not control connections to the RPC server in Sanctuary Application Server, see 'MaxRpcCalls' for that. Minimum: 0, maximum: 50000 (arbitrary). See 'Port', 'TLSPort', and 'TLSMaxSockets'. See also <a href="#">Table B.6</a> & <a href="#">Table B.7</a>	5000
Port	The TCP port on which the socket-based Sanctuary Application Server listens for new connections. Minimum: 1, maximum: 65534. This affects only clients. The port used by the RPC server (for administration clients) is controlled by the 'Protocols' setting. Minimum: 1, maximum: 65534. Transmissions that do not use the TLS protocol are always signed. See 'TLSPort', 'TLSMaxSockets', and 'MaxSockets'.	65129
RpcProtectionLevel	Determines whether the RPC (Remote Procedure Call) server will require RPC clients to identify (authenticate). Valid levels are: <ul style="list-style-type: none"><li>• '0': Instructs the OS to pick a protection level. At the time of this writing, this is equivalent to '2'.</li><li>• '1': No protection. Should not be used except for testing.</li><li>• '2': The client's identity is verified when connecting to Sanctuary Application Server. RPC messages are vulnerable to tampering and man-in-the-middle attacks.</li><li>• '3': For the connection-oriented protocols (TCP, for instance), same as '4'. For connectionless protocols (UDP), this level ensures that a client's connection cannot be hijacked at the request level.</li><li>• '4': Examines client credentials not only once per request (like '3') but with every single packet.</li><li>• '5': Like '4', with added cryptographic signing of every packet to defend against tampering.</li><li>• '6': Like '5', but also encrypts data in both directions.</li></ul> The recommended setting is '5' or more. Note that any setting except '0' requires the client to be in the same domain as the server, or in a domain that is trusted by the server's domain.	6



**Table B.5** Sanctuary Application Server registry keys (security registry keys)

Key name	Description	Default
SecureInterSxs	If set to 'yes', all inter-Sanctuary Application Server traffic is done using the TLS protocol. Note that Sanctuary Application Servers register the fully qualified DNS name in the servers table (for compatibility with older versions) and, depending on the communication mode selected, the TLS or the non-TLS port. Servers with different Inter-Sanctuary Application Server modes will not be able to communicate between them - they should either all have the 'yes' or 'no' value set for this parameter. When this value is set to 'no', communication is done using non-TLS ports. When setting this value to 'yes', you should also set the number of non-TLS sockets ('MaxSockets', see <a href="#">Table B.6</a> & <a href="#">Table B.7</a> ) to zero and 'CommVer' to '3' (clients v4.1 or later) to obtain the maximum level of security.	no
SndPort	The TCP port on which the Sanctuary Client is expected to listen. If absent or zero, 33115 is used. Minimum: 1, maximum: 65534.	33115
SxdConnectTimeoutMSec	The time, in milliseconds, that Sanctuary Application Server waits for the Sanctuary Client to accept a TCP connection. It is useful to keep this time as low as possible, but not so low as to impede connectivity. In a lightly loaded LAN, one second (1000 ms) should be quite ample. The value should be between 500 and 120,000 ms if it is out of these limits, the default value (5,000 ms) is used instead. **	5000
SxdPort	The TCP port on which the Sanctuary Client built-in server is expected to listen. If absent or zero, 33115 is used. Minimum: 1, maximum: 65,534.	33115
TLSTMaxSockets*	The maximum number of TCP connections that are allowed at any one time when using TLS protocol. See description on MaxSockets. Minimum: 0, maximum: 50000 (arbitrary). See 'Port', 'TLSPort', and 'MaxSockets'. See also <a href="#">Table B.6</a> & <a href="#">Table B.7</a> .	5000
TLSPort	The TLS port on which the socket-based Sanctuary Application Server machine listens for new connections. Minimum: 1, maximum: 65534. This affects only clients. Minimum: 1, maximum: 65534. Transmissions using TLS protocol are always encrypted. See 'Port', 'TLSTMaxSockets', and 'MaxSockets'.	65224
** See note on next section.		



The next table describes the configuration rules that follow the TLSMaxSockets and MaxSockets parameters (as described in the previous table) — see also [Table B.7](#):

**Table B.6** Configuring MaxSockets and TLSMaxSockets

TLSMaxSockets and MaxSockets values	Description
TLSMaxSockets > 0 AND MaxSockets = 0	Only TLS connections are available for Sanctuary Application Server-Sanctuary Client communication using the port specified on 'TLSPort'
TLSMaxSockets = 0 AND MaxSockets > 0	Only non-TLS connections are available for Sanctuary Application Server-Sanctuary Client communication using the port specified on 'Port'
TLSMaxSockets > 0 AND MaxSockets > 0	Both TLS and non-TLS connections are available for Sanctuary Application Server-Sanctuary Client communication using the ports specified on 'Port' and 'TLSPort'





Several registry keys (SecureInterSxs, CommVer, TLSMaxSockets, MaxSockets. Port, and TLSPort) interact together and some combinations are not valid as shown in the following table:

**Table B.7** Configuring SecureInterSxs, CommVer, TLSMaxSockets, MaxSockets. Port, and TLSPort

Secure InterSXS	Comm Ver	TLSMaxSockets	MaxSockets	Result	Notes
no	<3	0	0	✗	You must set the Non TLS Clients Max Concurrence field to a value >0 when selecting an older client protocol.
		0	>0	✓	Sanctuary Application Server - Client and intra-Sanctuary Application Server communication will be done using a non-TLS channel, This is only recommended when you already have an older installation and you are updating it.
		>0	0	✗	You must set the Non TLS client Max Concurrence field to a value >0 since you did not select the Secure Inter-Sanctuary Application Server option.
		>0	>0	✓	You should already have a valid computer certificate. Only used for migration purposes (updates) and not recommended for a new installation.
	3	0	0	✗	The selected protocol is 3: TLS is a requirement.
		0	>0	✗	The selected protocol is 3: TLS is a requirement.
		>0	0	✗	You must first select the Secure Inter-Sanctuary Application Server option.
		>0	>0	✓	You should already have a valid computer certificate. Only used for migration purposes (updates) and not recommended for a new installation.



**Table B.7** Configuring SecureInterSxs, CommVer, TLSMaxSockets, MaxSockets. Port, and TLSPort

Secure InterSXS	Comm Ver	TLSMaxSockets	MaxSockets	Result	Notes
yes	<3	0	0	✗	You cannot select the Secure Inter-Sanctuary Application Server option when the TLS Clients Max Concurrence field is set to a value = 0.
		0	>0	✗	You cannot select the Secure Inter-Sanctuary Application Server option when the TLS Clients Max Concurrence field is set to a value = 0.
		>0	0	✓	You should already have a valid computer certificate.
		>0	>0	✓	You should already have a valid computer certificate. Only used for migration purposes (updates) and not recommended for a new installation.
	3	0	0	✗	The selected protocol is 3: TLS is a requirement.
		0	>0	✗	The selected protocol is 3: TLS is a requirement.
		>0	0	✓	You should already have a valid computer certificate.
		>0	>0	✓	You should already have a valid computer certificate. Only used for migration purposes (updates) and not recommended for a new installation.

The entries in the table below are found within the following key:

HKLM\system\CurrentControlSet\Services\EventLog\Applications\sxs

**Table B.8** Sanctuary Application Server registry keys

Key name	Description	Default
EventMessageFile	Path and file name of SXS.EXE.	
ReportMaxRecords	Maximum number of records a report will contain.	10000
ReportGenerationTimeout	Cancel the report generation of a report, if it is not possible to generate it within a specific time. The timeout is in milliseconds.	12000
ReportThreads	Number of threads to use. A default of 0 implies two threads per processor.	0



**Table B.8** Sanctuary Application Server registry keys

Key name	Description	Default
ReportStoragePath	A path Sanctuary Application Server will use for temporary storage.	sxsdata
TypesSupported	Supported message for the event log. 0x10 for AUDIT_FAILURE and 0x08 for AUDIT_SUCCESS (value is of type REG_DWORD). You can combine the values in a hexadecimal addition. The default value (0x1F) stands for: Register all type of messages. Other values are: 0x00Success 0x01Error 0x02Warning 0x04Information 0x08Success 0x10Failure	0x1F

## Sanctuary Client Registry Keys

The changes to the registry values are only effective after a reboot of the client computer. Sanctuary Command & Control, SCC, is in charge of all communication between server, client(s), and the CA server. Its keys are located in `HKLM\system\CurrentControlSet\Services\scomc\parameters`.

The following table contains details of each registry key entry for SCC (all these entries are of type REG\_SZ; string value):

**Table B.9** Client registry keys (1/2)

Key name	Description	Default
CertGeneration	'yes' means that the client is in 'automatic' mode and request the needed certificate. 'no' means that the client in 'manual' mode, the certificate has to be generated manually.	Defined during client installation.
Debug (optional)	Use for debugging purposes.	3 (you must reboot in order to make it work).
FirstServer (optional)	If this is greater than or equal to the number of IP addresses in the list located on the Servers key, Sanctuary Client will use this value as a zero-based index into the list. If a server cannot be contacted, the next one is used, in a round-robin fashion. If the key is missing or has a -1 value, existing servers are randomly chosen.	n/a



**Table B.9** Client registry keys (1/2)

Key name	Description	Default
HardeningMode	Displays the level of permissibility allowed to modify, repair, or remove the client, registry keys, or special directories (disabled, basic, or extended). **	disabled
HardeningStatus	Displays if the Hardening Mode is taken or not into consideration. **	inactive
HID\*	Internal use. Do not modify.	n/a
HistoryPeriodSecs (optional)	Internal use. Do not modify.	n/a
ImportDir	The directory used to import the policies file.	C:\Program Files\Lumension Security\Sanctuary\Import
LastSeenComputerName	Internal use. Do not modify.	n/a
LastShadowUploadTime	Indicates the last time the shadow update was done. The update consists on copying the file data or name, depending on the shadowing rule, from the client computers.	n/a
LastSxLogUploadTime	Indicates the last time logs were transmitted.	n/a
Log file name	Gives the name of the log file written if 'Log to file' is 'yes'.	'scomc.log'
Log to console	If 'yes' or '1', sends debug messages to the console, if any.	no
Log to dbwin	If 'yes' or '1', sends debug messages to Dbwin32.	no
Log to file	If 'yes' or '1', sends debug messages to the log file (see below).	no
Salt	An internally generated 15-byte random value used for protection purposes. It is calculated when the client starts.	n/a
Servers	A list of Sanctuary Application Server names (FQDN) or IP addresses, separated by spaces. A port number may be specified for any server by appending a colon and the port number to the name/address of the server (e.g. '10.34.22.16:65129 sxs.example.com:65130').	Those defined during the client installation.
ServersOverride	Internal use. Do not modify.	n/a
ShadowDirHistory (optional)	Internal use. Do not modify.	n/a
TicketDir	Directory where the endpoint maintenance ticket has to be copied in order to relax 'client hardening'.	n/a



**Table B.9** Client registry keys (1/2)

Key name	Description	Default
UseTLS	'yes' when TLS is used (all communication is encrypted) 'no' when TLS is not used (all communication is signed).	Defined during client installation.
TcpConnTimeout	Defines the default connection timeout the client uses when importing policies and permissions from a file:  If not present 3 minutes is used. If an incorrect value or a value less than 30,000 milliseconds (30 seconds) is provided, then 30 seconds is used  When used for exporting setting from the management console you should define the same registry key but in: SOFTWARE\Lumension Security\smc\	Value in milliseconds
<b>**Note:</b> This registry key does not controls client hardening itself, it is for information purposes only.		

The following table contains details of the major registry key entries for Sanctuary Client Kernel.

The Parameters subentry is used to save different program options. Its keys are located in:

HKLM\system\CurrentControlSet\services\sk\parameters

**Table B.10** Client registry keys (2/2)

Key name	Type	Description	Default value
Enum	Subkey	Contains device list. *	n/a
Limits	Subkey	Copy limit settings (UpdateTime, CachedSize, and so on). *	n/a
EventLog	REG_DWORD	Internal use. *	n/a
FileLog	REG_DWORD	Internal use. *	n/a
Classes	REG_DWORD	Contains device names and permissions. *	n/a
HistoryPeriodSecs	REG_DWORD	Internal use. *	n/a
ShadowDirHistory	REG_BINARY	Internal use. *	n/a
Debug	REG_DWORD	Use for debugging purposes.	3 (reboot to activate)
Security	Subkey	Internal use. *	n/a
ComputerName	REG_SZ	Internal use. *	n/a
*Do not modify			



## Sanctuary Management Console

---

The following table contains details of the registry key entry that controls various aspects of how the management console interface works.

The key is located in:

HKEY\_CURRENT\_USER\Software\Lumension Security\Sanctuary\

**Table B.11** Console registry keys

Key name	Type	Description	Default value
ForceLCID	DWORD	Defines the console's interface language: <ul style="list-style-type: none"><li>• 1033 English</li><li>• 1031 German</li></ul>	1033



# C Upgrading from Old Versions

The information in this appendix is product specific.

If you are upgrading from a previous version of Sanctuary, you should be aware that the upgrade process should always be done in the following order:

1. If you are using any of the programs that form our Sanctuary Application Control Suite, you have to ensure that the computer and user/group 'Blocking Mode' option is set to the appropriate unblocking value. If this is not done, the setup cannot proceed, as it would be classified as an unknown executable that needs authorization.
2. Stop the Sanctuary Application Server service. This service can be started and stopped through the Windows Services Panel or using the command line (`net stop sxs` and `net start sxs`). The setup Wizard stops, updates, and starts the service automatically without your intervention only if the Sanctuary Application Server resides on the same machine as the Sanctuary Database. If you are using several Sanctuary Application Server please stop their respective services manually before proceeding.



**Note:** We strongly recommend backing up your database before updating Sanctuary.

3. Update the Sanctuary Database in your SQL server (SQL Server 2000 SP4/2005 SP2, or SQL Server 2005 Express Edition SP2).
4. Update all existing Sanctuary Application Server.
5. Update the Sanctuary Management Console.
6. Finally, update the Sanctuary Client(s).



**Warning:** Old Sanctuary Management Consoles simply refuses to communicate with a more recent Sanctuary Application Server.



**Warning:** A Sanctuary Client update requires a reboot.



**Warning:** Never change the key pair during a Sanctuary upgrade where client hardening is switched on, otherwise your upgrade will fail.





**Note:** If you update from older versions of Sanctuary, but you keep the old clients, device/application permissions are NOT sent to them. You must consider updating these older clients as soon as possible. You also lose the added security that new Sanctuary Client offers against deleting, modifying, or altering its components.



**Note:** You must stop Sanctuary Application Server(s) — using ‘net stop SXS’ from the command-line prompt — **before** updating the database.



**Note:** If you are planning to keep old clients versions, do not forget to choose the correct communication protocol supported by your Sanctuary Client when updating your Sanctuary Application Server(s).



**Note:** You must have a Certificate Authority if you want to take advantage of an encrypted channel for Sanctuary Client -Sanctuary Application Server and intra-Sanctuary Application Server communications.

To summarize, the upgrade is done in two broad stages:

- First, upgrade all server-side components – during this first stage, the new server-side components have to work with the old client versions.
- Second, deploy the new client upgrade packages – the client deployment stage may be organized in batches and may take several days to complete.

The server-side components have not been designed to communicate with old clients (older than version 3.x). You should also update them.

## Sanctuary Device Control

---

Sanctuary installation routines can upgrade from Sanctuary Device Control version 3.0 and above. If you are running an older version, you should first **uninstall the program completely** before deploying the new server and client components.





**Note:** Since permission's structure has changed radically from previous versions, your risk not transmitting them properly to older clients. You should consider an immediate client update in these cases.



**Note:** You may have to manually re-classify some devices in other classes. This is specially true if the class they belong to has been reclassified or disappear. Please check the Sanctuary Device Control User Guide and the readme file for more info.

## Sanctuary Server Edition

---

Sanctuary installation routines support upgrading from version 3.x. If you have a previous version, you should first **uninstall it completely** before deploying the new server and client components.

## Upgrading Server-side Components

---

1. If you have installed the Sanctuary Application Server on a different computer than the database, it is important that you stop the Sanctuary Application Server service on that computer before upgrading:  
  
`net stop sxs`
2. Run the setup.exe file located in the \SERVER\db folder on the computer where you installed the Sanctuary Database.



**Warning:** You should do a database backup before proceeding with an update

3. Run the setup.exe file located in the \SERVER\SXS folder on the computer(s) where you installed the Sanctuary Application Server.

Run the setup.exe file located in the \SERVER\SMC folder on the computer(s) where you installed the Sanctuary Management Console.





**Note:** It is very important that you upgrade first the database, then the Sanctuary Application Server(s), and finally the Management tools. Furthermore, always upgrade server-side components before upgrading the clients.

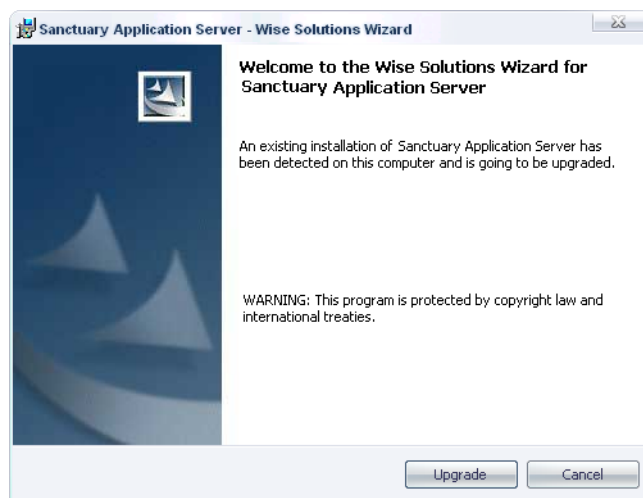
### Upgrading from a Previous Sanctuary Application Server Version

---

If you are upgrading the Sanctuary Application Server instead of making a 'clean' installation, the dialogs and steps change from those found in the Sanctuary Application Server installation chapter as depicted in the following steps.

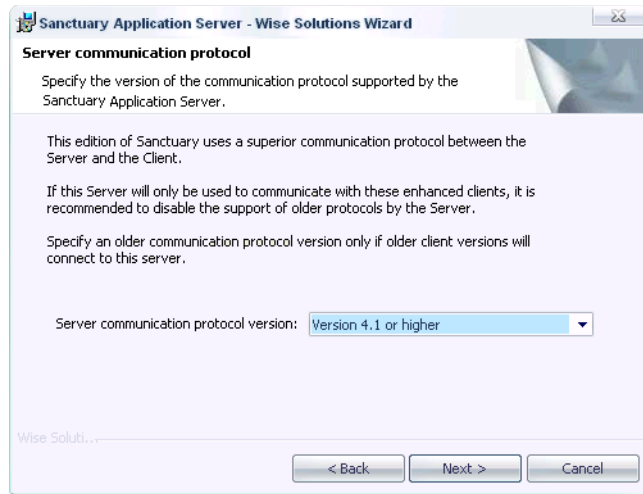
1. Log on to the computer where the Sanctuary Application Server component is installed.
2. Close all programs running on the computer and stop the Sanctuary Application Server service (Net Stop SXS).
3. Insert the Sanctuary CD in your DVD/CD drive and run `\SERVER\sxs\setup.exe`.

The *Welcome* dialog is displayed informing you that a previous version of the server is already installed and there is an upgrade.



**Figure C.1** Sanctuary Application Server upgrade: First step

4. Click *Next* to continue. You are now asked what kind of communication protocol the Sanctuary Application Server should use.  
You can choose among:
  - v3.1 or older
  - v4.0 or older
  - v4.1 or newer.
5. Choose your option from the list. You can always change this setting later by modifying the CommVer registry key — see [Table B.8](#) on page 162 for more information.

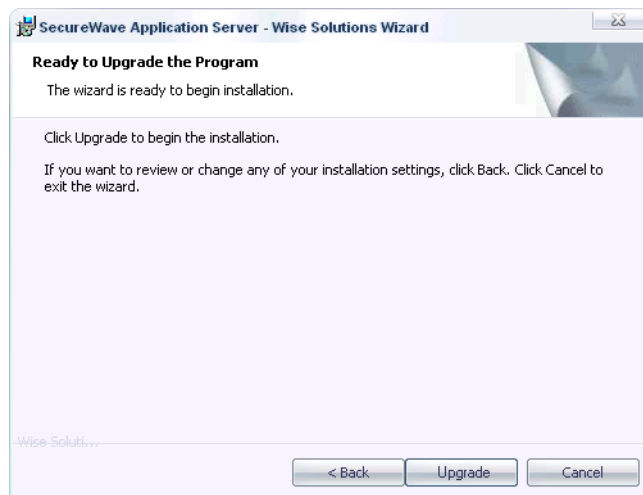


**Figure C.2** Sanctuary Application Server upgrade: Protocol selection dialog

6. Choose to upgrade or keep your old log templates.



7. The setup program has now all the necessary elements to begin the installation or upgrade process.

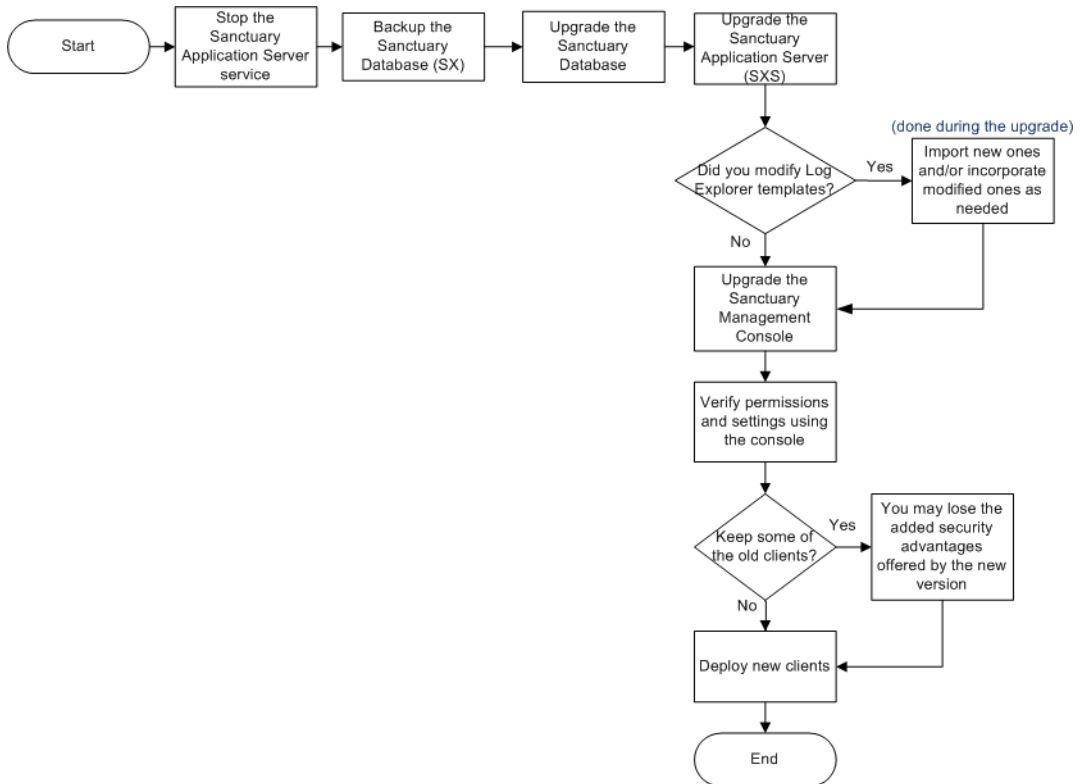


**Figure C.3** Sanctuary Application Server upgrade: Protocol selection dialog

8. Click *Upgrade* to begin the process.
9. The program verifies your license and RPC protocol.

## Upgrading Guideline

You can use the following flowchart as a general guideline when updating your Sanctuary product. Nevertheless, you should ALWAYS refer to the appropriate section before attempting an upgrade.



**Figure C.4** Upgrade flowchart





# D Installing Sanctuary Components on Windows XP/2003/Vista

The information in this appendix is relevant to all Sanctuary software suite products.

Throughout this chapter we refer to Windows XP, Windows 2003, and Windows Vista. When we refer to these operating systems, we are explicitly (unless otherwise noted) referring to their latest service packs:

- Windows XP (SP2 or later)
- Windows 2003 (SP1 or later)
- Windows Vista (SP0 or later)

By default, Windows Firewall is enabled on computers that are running Windows XP, Windows 2003, or Windows Vista. Windows Firewall closes ports such as 33115, 65129, and 65229 (if using TLS protocol) that are used by Sanctuary Client and Sanctuary Application Server to communicate over TCP. Sanctuary Clients that are trying to connect to the Sanctuary Application Server will not be able to connect until an exception is set in Windows Firewall.

With these Service Packs, a number of changes have been made in the Remote Procedure Call (RPC) service that help make RPC interfaces secure by default and reduces the attack surface of Windows XP/2003/Vista. Sanctuary Management Console installed on Windows XP/2003 trying to connect to the Sanctuary Application Server will not be able to do so unless the appropriate options are set.



**Warning:** Although you can use Windows XP/2000 Pro/Vista for the database or/and console, you should not use it for the Sanctuary Application Server (or Sanctuary Client in the case of Sanctuary Application Control Server Edition).

## Connection Between Sanctuary Application Server and the Sanctuary Database

The Sanctuary Application Server uses the MDAC (Microsoft Data Access Components) to connect to Sanctuary Database.

ADO (Microsoft ActiveX Data Objects), the technology used by the Sanctuary Application Server, relies on a protocol called Tabular Data Stream (TDS). By default, TDS uses port 1433 for incoming database traffic.

When the Sanctuary Database is installed on a Windows XP/2003/Vista computer, make sure that the TCP port 1433 is opened. Please refer to “[Configuring the Firewall](#)” on page 179 for information about how to configure Windows XP/2003.



You can preset the TDS port to another one during SQL Server setup (when you select the *Select Network Protocols* option). After you have installed SQL Server, you must rerun the setup program and select the *Change Network Support* option to change the TDS port.

If you want to use another port instead of the standard one (1433), you need to create an Alias. To do this, follow these steps:

1. Use the Client Network Utility command found in the *Start Programs → Microsoft SQL Server* menu.
2. The *SQL Server Client Network Utility* dialog is displayed.
3. Choose the *Alias* tab.
4. Click on **ADD**. The *Add Network Library Configuration* dialog opens.
5. Type in a name in the 'Server Alias' field. If you are using Network Libraries, select the *TCP/IP* option.
6. Type in the *Server name* and change the port in the lower field (*Pipe name*) located on the right panel of the dialog (*Connection parameters*).
7. Click on **OK** to close the dialog and accept the new Alias.

During the setup process, you must then provide this Alias instead of the SQL server name.

You can find more details, in the Microsoft knowledge base article 'How Windows XP Service Pack 2 (SP2) Affects SQL Server and MSDE 2000', available at the Microsoft's Web site.

## Connection Between the Sanctuary Management Console and the Sanctuary Application Server

---

A number of changes have been made in the Remote Procedure Call (RPC) service for Windows XP/2003/Vista that help make RPC interfaces secure by default and reduce the attack surface on these operating systems. The most significant change is the addition of the **RestrictRemoteClients** registry key. This key modifies the behavior of all RPC interfaces on the system and, by default, eliminates remote anonymous access to RPC interfaces, with some exceptions.

The Sanctuary Management Console uses the RPC protocol to connect to the Sanctuary Application Server.

Please note that there have been several important changes concerning the TCP/IP communication protocol, RPC, firewall, and other points since Windows XP SP2. Please refer to Microsoft's Web site for more information.

### Stage 1: Configuring a Fixed Port on the Server

By default, Sanctuary Application Server uses dynamic ports for the RPC communication with the Console. The ports change every time the Sanctuary Application Server is started, making it impossible to configure the firewall.





In order to be able to configure the firewall, it is mandatory to instruct the Sanctuary Application Server to use a fixed port. To do this, open *RegEdit* and set the following entry:

```
Key: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services
\sxs\parameters
Name: Protocols
Type: REG_SZ
Value: 'ncacn_ip_tcp[1234]'
```

where 1234 represents the fixed TCP port number that you want to use for the communication between the Consoles and the Sanctuary Application Server.

You should restart the Sanctuary Application Server for the setting to take effect (using the line commands `net stop sxs` and `net start sxs`).

## Stage 2: Opening the Port on the Server Firewall

On the computer where the console is installed, open the chosen ports on the firewall. If you have the console installed on Windows XP/2003/Vista, see [“Configuring the Firewall”](#) on page 179 for more details.

## Connecting to the Server Using the Fixed Port

In the *Connect* dialog of the Sanctuary Management Console, specify the fixed port to use to communicate with the server, such as `secsrv.secure.com[1234]`.

## Connecting Using the Endpoint Mapper

If you do not want to specify the fixed port in the *Connect* dialog of the Sanctuary Management Console, it is possible to instruct the Console to retrieve the port in use directly from the Endpoint Mapper on the Sanctuary Application Server.

In Windows XP, 2003, or Vista by default, the RPC Endpoint Mapper interface (port 135) is not accessible anonymously. This is a significant security improvement, but it changes the task of resolving an endpoint.

Currently, an RPC client that attempts to make a call using a dynamic endpoint first queries the RPC Endpoint Mapper on the server to determine to which endpoint it should connect. This query is performed anonymously, even if the RPC client call is, itself, done using RPC security.

Anonymous calls to the RPC Endpoint Mapper interface fail by default on Windows XP, Windows 2003, or Windows Vista because of the default value for the `RestrictRemoteClients` key.

This makes it necessary to modify the RPC client runtime to perform an authenticated query to the Endpoint Mapper. If the `EnableAuthEpResolution` key is set on the client, the RPC client runtime uses NTLM to authenticate to the Endpoint Mapper.



Setting the EnableAuthEpResolution Registry Key instructs the Sanctuary Management Console to use NTLM to authenticate to the Endpoint mapper and obtain what endpoint it should connect to on the Sanctuary Application Server.

You may also experience some authentication problems when running the Sanctuary Management Console on a computer with Windows XP, 2003, or Vista. The console displays an access denied popup message even when the correct credentials are specified. To fix this, the following key must be set on the Windows XP, 2003, or Vista machine(s) running the Sanctuary Management Console:

Key: HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\RPC

Name: EnableAuthEpResolution

Type: REG\_DWORD

Value: 0x00000001

and

Name: RestrictRemoteClients

Type: REG\_DWORD

Value: 0x00000000

See <http://www.microsoft.com/technet/prodtechnol/winxp/opro/maintain/sp2netwk.msp> for more information about these settings.



**Note:** The Sanctuary Management Console setup prompts you to create this key if it does not exist.



**Note:** Operating systems prior to Windows XP SP2/2003 SP1 do not support the 'EnableAuthEpResolution' key.

## Summary

The following table summarizes the communication ports and registry keys used in Sanctuary:

**Table D.1** Communication ports in Windows XP

Connection string to use in the Sanctuary Management Console	Port to open on the Sanctuary Application Server firewall	Protocols registry key on the Sanctuary Application Server
MyComputer.MyDomain.com[1234]	1234	ncacn_ip_tcp[1234]
MyComputer	1234 & 135	ncacn_ip_tcp[1234]
<b>Note:</b> Replace '1234' with the actual port you want to use for the communication between the Sanctuary Management Console and the Sanctuary Application Server.		

## Connection between the Sanctuary Client and the Sanctuary Application Server

If you install the Sanctuary Application Server and the client(s) on different machines, and you have a firewall between them (including Windows XP firewall, if applicable), the communication between them may be blocked.

The default ports used for the communication between the drivers and Sanctuary Application Server are the following ones:

- The Sanctuary Application Server listens on port TCP 65129 (65229 if using TLS protocol).
- The Sanctuary Clients listens on port TCP 33115.

See the next section, [“Configuring the Firewall”](#), for information about how to configure Windows XP/2003/Vista.



**Note:** You can also manually configure the ports used for the communication between the client and the Sanctuary Application Server. See [“Sanctuary Application Server Registry Keys”](#) on page 153 and [“Sanctuary Client Registry Keys”](#) on page 163.

## Configuring the Firewall

Since Windows XP SP2 and Vista SP0, the integrated firewall is enabled by default. You can also activate it on Windows 2003 SP1 (or later). Here is a procedure to open a TCP port on the firewall:

1. Click on *Start*, and then click *Run*.



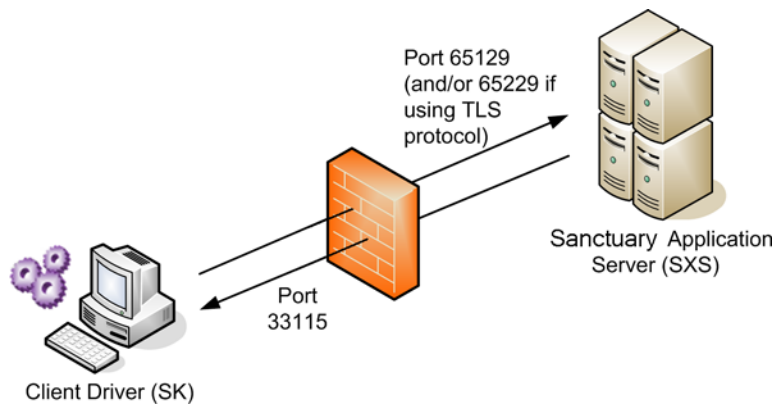
2. In the *Run* dialog box, type *Firewall.cpl*, and then click *OK*.  
On Windows Vista click *Change Settings* first.
3. On the *Exceptions* tab, click *Add Port*.
4. In the *Port number* box, type the number of the port to open (33115, 65129, and 65229 — if using TLS protocol), and then click *TCP*.
5. In the *Name* box, type a name for the port, and then click *OK*. The new service is displayed on the *Exceptions* tab.
6. To enable the port, click to select the check box next to your new service, and then
7. Click *OK*.



**Note:** The Installation Wizard proposes to open these ports for you during the setup phase even if they are already opened.

Another way of configuring your firewall is by using Windows' *Netsh* command. To open a port using this command:

1. Click *Start*, and then click *Run*.
2. In the *Run* dialog box, type '*netsh firewall set portopening TCP 33115 Lumension\_33115 ENABLE*', and then click *OK*. In this example, we use port 33115 and name the rule "Lumension\_33115". You will also need to open port 65129 and 65229 (if using TLS protocol).



**Figure D.1** Communication ports between Sanctuary Application Server and the client

# E Opening Firewall Ports for Client Deployment

The information in this appendix is relevant to all Sanctuary software suite except for Sanctuary Application Control Server Edition (as the client cannot be installed on Windows XP, Windows 2000 Pro, or Windows Vista computers).

Microsoft Windows XP SP2 and Vista enables the Windows Firewall by default. While this firewall configuration helps secure your system, it can also prevent legitimate software from interacting with the computer.

Many NetBIOS and DirectHost services, such as our deployment tool, rely upon a combination of TCP and UDP network ports, specifically TCP 139, TCP 445, UDP 137, and UDP 138. These services are installed by default on Windows NT 4.0 and Windows 2000 systems, as well as domain-joined Windows XP systems.

With the advent of Windows XP SP2 and Vista these services are, by default, no longer available to remote systems. This firewall denies access to these services and prevents connections to all network ports. The defaults settings prevent our installation tool to connect to the remote computers.

With the methods described in this appendix, you can preserve system security while deploying our software in your organization.

You can apply these necessary firewall settings on a computer-by-computer basis, or via an Active Directory domain group policy as explained in the following sections.



**Note:** You should activate the 'File and Print Sharing to Microsoft Networks' & 'Client for Microsoft Networks' services in all your machines. These services are used for the Sanctuary Client deployment, eDirectory synchronization, and if you are planning to install SQL Server 2005 Express Edition SP2.

## To Manually Open the Ports on a Computer-by-Computer Basis

1. *Start* → *Settings* → *Control Panel* → *Windows Firewall* (or click on SECURITY CENTER and then WINDOWS FIREWALL) and go to the *Exceptions* tab.

On this tab, you can choose to enable the *File and Print Sharing services* (as well as other listed services). By enabling File and Printer Sharing services, TCP ports 139 and 445, and UDP ports 137 and 138, you can install our client remotely using our deployment tool, while all other (non-selected) services are blocked.

If the computer resides on a remote IP subnet, you will need to edit the service and choose Subnet as the Scope.

2. Click on OK to close the Windows Firewall control panel.



3. Restart the computer to enable these choices.

### To Open the Ports on a Computer-by-Computer Basis with a .bat File

---

Open your notepad or your favorite text processor and type or copy and paste the following lines:

```
netsh firewall set portopening protocol=UDP port=137  
name=Sanctuary_UDP_137 mode=ENABLE profile=All  
netsh firewall set portopening protocol=UDP port=138  
name=Sanctuary_UDP_138 mode=ENABLE profile=All  
netsh firewall set portopening protocol=TCP port=139  
name=Sanctuary_TCP_139 mode=ENABLE profile=All  
netsh firewall set portopening protocol=TCP port=445  
name=Sanctuary_TCP_445 mode=ENABLE profile=All
```

Save and run on each machine.

### To open the Firewall Ports via an Active Directory Group policy

---

While it is possible to open ports manually in a small network, this can also be achieved in a larger scale by centrally configuring the Windows firewall using Group Policy. When the XP (SP2 or later)/Vista machines log on to the network, they will inherit the customized Group Policies, thus opening the Windows Firewall ports required for remote deployment. This is the Microsoft recommended method to centrally manage Windows Firewall settings.

In the following steps, we modify a domain group policy to open the needed ports.



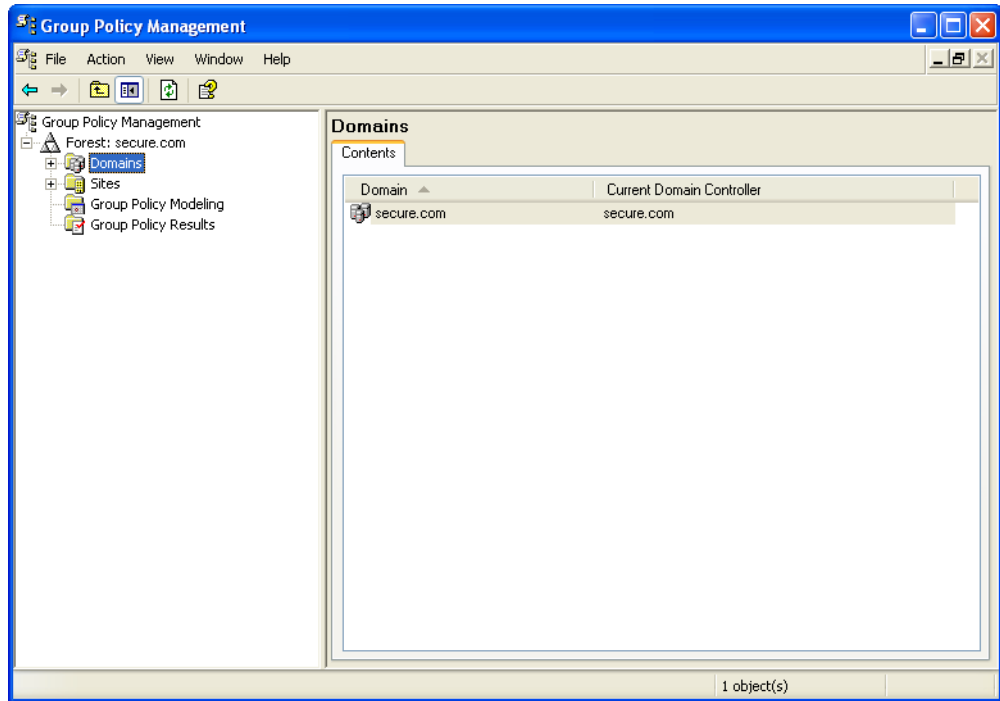
**Note:** To avoid compatibility problems ensure that the machine has the latest patches and service packs.

If you are using a Windows Server 2003 with Service Pack 1 (or later) computer joined to the domain:

1. Log on as domain administrator.
2. Download and install the .NET framework (required for the next step).
3. Download and install the Microsoft Group Policy Management Console (GPMC) from Microsoft's Web site.

## To Create the Group Policy (GPO)

1. Open the Group Policy Management console (*Start Run → gpmmc.msc*)



**Figure E.1** Open firewall ports: Select domain and forest

2. Select the Forest and the Domain for which you want to create a Windows Firewall Policy.



- 3. Right-click on the entry for *Default Domain Policy* and select EDIT.

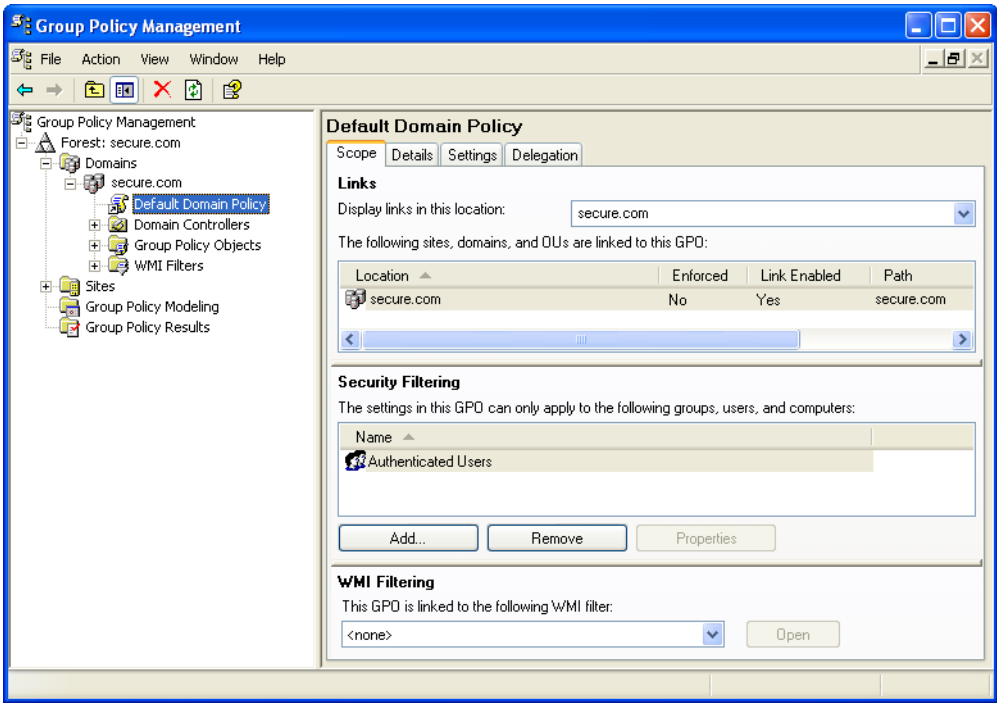
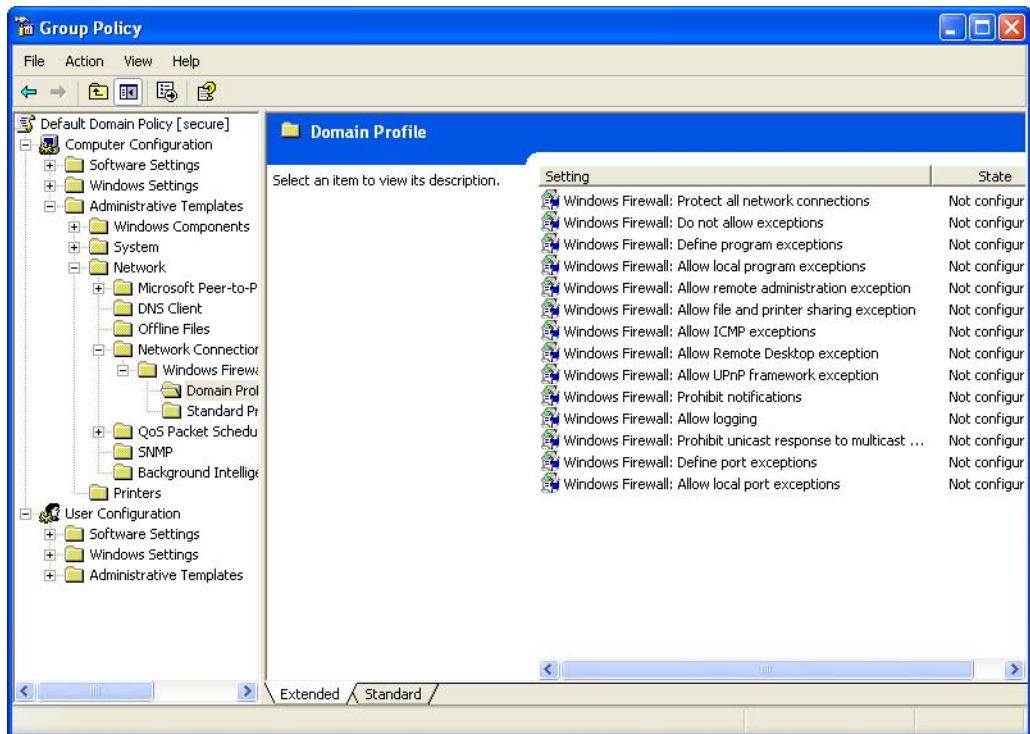


Figure E.2 Open firewall ports: Edit the Default Domain Policy





This opens a *Group Policy* window for the selected domain:



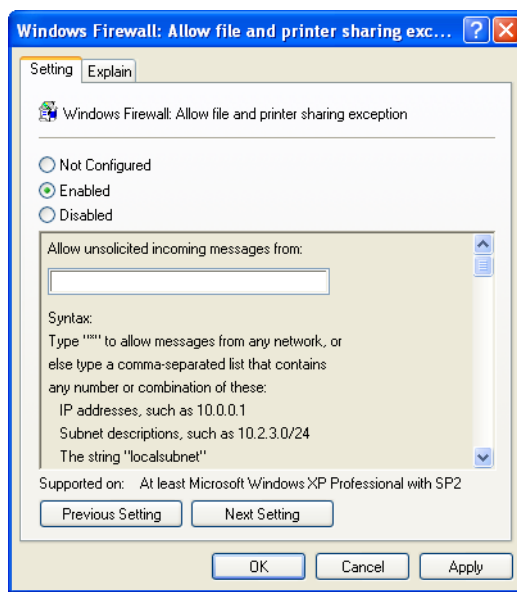
**Figure E.3** Open firewall ports: Modify file and printer sharing exceptions

4. Expand the *Computer Configuration* tree and navigate to the *Administrative Templates* → *Network* → *Network Connections* → *Windows Firewall* → *Domain Profile* folder, as illustrated in the previous figure.

The simplest way to enable the ports used by our deployment tool is to enable the policy *Windows Firewall: Allow file and printer sharing exception*.



5. Right-click on *Windows Firewall: Allow file and printer sharing exception* and select *Properties*. The following dialog appears:



**Figure E.4** Open firewall ports: Enable the required ports

6. Choose *Enabled* and then enter *Localsubnet* in the *Allow unsolicited incoming messages from* field.
7. To save these settings click on *APPLY* and then on *OK*.

Enabling File and Printer Sharing access opens TCP ports 139 and 445, and UDP ports 137 and 138, making them available to other machines on the same local IP subnet. These machines appear completely blocked for systems outside of the local subnet.

## To Improve Security

To enhance further the security, you can replace 'localsubnet' in step 6 of the preceding procedure with the specific IP address or addresses (comma separated) of the computers allowed to deploy the client.

# F Using the Synchronization Script for Novell

The information in this appendix is relevant to all Sanctuary products. When using Sanctuary Application Control Server Edition, be aware that the client cannot be installed on Windows XP, Windows 2000 Pro, or Windows Vista computers, you will be limited to an installation in a Windows Server 2003.

## Introduction

Novell has always been an active part of the network community. Its roots go back to the early 1980s when it offered a product to share files and printers in a small LAN structure based on PCs. Still going strong today, Novell networks have the same security and data control problems as all other LAN and WAN products in the market. Many modern WANs and LANs share different network operating systems in a heterogeneous environment that often include Novell as a solution.

In this appendix, we analyze the extra component offered by Sanctuary to synchronize those eDirectory objects (OU, group, user, and workstations) so that an administrator can manage them and deny/allow access to I/O devices in a Novell setting.



**Note:** You should activate the 'File and Print Sharing to Microsoft Networks' service & 'Client for Microsoft Networks' in all your machines. These services are used for the endpoint driver deployment, eDirectory synchronization, and if you are planning to install SQL Server 2005 Express Edition SP2.

## What Components are Required?

There are four distinct components necessary for the implementation of Sanctuary on Novell systems:

- A Novell server (version 6.5 or later, version 5.x requires Lumension approval).
- A SQL server that holds the Sanctuary Database — it does not need to have a Novell client, but it may if you are trying to run the synchronization script directly from the server so you do not need to specify the SQL address, user name and password.
- A Sanctuary's script file (written in VBScript) provided on the installation CD under the \scripts directory.
- A Windows machine with a Novell client on which the synchronization script is executed. This machine must already have Novell's NDAP ActiveX objects installed. You can find these components on Novell's Web site or on your Sanctuary installation CD.



## How does the Novell Interface Works?

Once Sanctuary is installed and configured completely — including the Sanctuary Application Server, Sanctuary Database, and Sanctuary Client — Novell’s eDirectory trees are synchronized using an external script and appear on the Sanctuary Management Console structure so that permissions and rules can be assigned to explicit objects. This VBScript translates and synchronizes the Globally Unique Identifiers (GUIDs) of eDirectory objects into the Security Identifiers (SID) used internally by Sanctuary.

The administrator can still use the *Synchronize Domain* command of the *Tools* menu (or from the *Control Panel*) to synchronize individual machines or Windows domains.

The administrator must run the synchronization script on a regular basis to synchronize all eDirectory objects. This can either be done manually or with a scheduled execution:

- In the manual execution, the administrator starts the VBScript by running it directly from the Windows’ Run menu or command window.
- For a scheduled execution, the administrator uses the Windows Task Scheduler Service (AT or WINAT). Please see “[Scheduling Domain Synchronizations](#)” on page 135 for an example.

## Synchronization Script Parameters

The script asks for four parameters, only one of which is mandatory:

**Table F.1** Novell script’s parameters

Parameter	Used for	Notes
Novell server tree name	Novell server’s tree name to be synchronized.	Compulsory.
SQL server address or name	The address or name of the SQL server hosting the Sanctuary Database.	Optional. If none specified, ‘(local)’ is used. This only works when Novell’s client, the synchronization script, NDAP, and the database are on the same physical machine.
User’s name	The user’s name used to log into the SQL database.	Optional. If none specified, a ‘blank’ user is used.
User’s password	The user’s password used to log the user into the SQL database.	Optional. If none specified, a ‘blank’ password is used.



The user's name and password used to connect to the Novell server are those of the logged one. Take into account that if you do not logon as administrator, you will not have access to some objects of the eDirectory tree. If the SQL credentials are not specified, the current ones are used instead.



**Note:** If you are using Microsoft SQL 2005 SP2 you should specify the SQL server (optionally the user name and password), even if it is local to the machine, as (local)\SQLEXPRESS. Example: `c:\>cscript.exe \path_to_folder\NDSSync.vbs Novell_Server_Tree (local)\SQLEXPRESS`.

## How to use Novell's Synchronization Script

---

Once all the Sanctuary components are installed —the Sanctuary Database, Sanctuary Application Server, and Sanctuary Management Console — make sure that the console can communicate with the Sanctuary Application Server and that the administrators can define or modify Sanctuary policies. Once this done, follow these simple steps:

1. Configure initial policies using the well-known accounts (Everyone, LocalSystem, etc).
2. Deploy Sanctuary Client.
3. The Sanctuary Clients must be able to communicate with the Sanctuary Application Server and they must adhere to the policies that apply to the well-known accounts.
4. Run the synchronization script, either manually or automatically.
5. Once the script finishes, the account selection dialogs in the console should display the user accounts, groups, and OUs.
6. Make the changes you want to the Sanctuary policies.
7. Update the clients and check whether they follow the new policies.



**Note:** Although any user can start the synchronization process, just like in the Active Directory case, some eDirectory objects may require additional permissions. This depends on the organization's structure and policy. The user must be the database owner or have insert+delete+update permissions to do the synchronization.



**Note:** Only user, group, OU, and Organization objects are synchronized. If ZENworks is installed, Workstation objects are also synchronized.



### Script Examples

---

In this section, we give some typical usage examples. Remember that you can always run the script through Windows' Scheduler Task.

1. `cscript.exe NDSSync.vbs Novell_server_tree`  
In this example, we are trying to synchronize objects from the Novell tree called 'Novell\_server\_tree' and place them on the local database SQL server. You will need to run it directly from the SQL server machine so you need Novell's client, synchronization script, NDAP and the database on the same physical machine. You can find these components on Novell's Web site or on your Sanctuary CD.
2. In the next example, the script is not run locally from the SQL server machine. You need to specify, besides the Novell server, the emplacement of the database server:  
`cscript.exe NDSSync.vbs Novell_Server_tree DB_server`
3. The next example explicitly sets the user and password to access the table in the database since they are not the same as the logged user who runs the script:  
`cscript.exe NDSSync.vbs Novell_Server_tree DB_server Authorized_user User's_Password`
4. If you want to save the results in a log file, you can use redirection characters:  
`cscript.exe NDSSync.vbs Novell_Server_tree > log.txt`



**Note:** Remember that you require Novell's client, the synchronization script, and NDAP on a Windows machine.

### What Can go Wrong and How do I Fix It?

---

In this section, you can find a general guidelines to some common errors found when running the script. We do not include the obvious ones such as not finding the script or using it directly instead of running it through `cscript.exe`.

#### **The script is not working or it is missing some objects in the eDirectory structure.**

Check that you have the correct permissions for the Novell server you are specifying. If you do not have administration rights, the script will fail to synchronize all/part of the eDirectory structure.

#### **I get the message 'DB connect failed'**

Check you are specifying the correct SQL server address, user's name and password. Ensure the SQL server is up and running. Check there is a valid connection between your machine and the SQL server (try troubleshooting using the PING command). Check that the database table (sx) has been correctly installed.

**I get the message ‘DBStart failed’**

Check you have the correct database rights. You must be a user, or specify the correct one as a parameter, that has insert+delete+update permissions for the database in order to do the synchronization.

**I get the message ‘DBFeedDomain failed’**

Several SQL statements failed to execute. Ensure you have the proper rights to insert+delete+update in the database table.

**I get the message ‘DBComplete failed’**

Several SQL statements failed to execute. Check you have the proper rights to insert+delete+update in the database table.

**There is no synchronization when running NDSSync.vbs script**

If you installed SQL Server 2005 Express Edition with our installation wizard, or manually using the Windows Authentication mode, you cannot connect to the Sanctuary Database machine using credentials different from those of the system administrator provided as script’s parameters. Login as administrator of the Database Server machine or enable SQL Authentication for your SQL Server 2005 Express Edition installation.

**I get the message “ActiveX component can’t create object: ‘NWDirLink.NWDDirCtrl.1’”**

Check that NDAP is installed on the machine from where you are running the script. If it is already installed, run Regocx.bat (found on your installation CD or on Novell’s Web site), on the Novell client machine which is used to synchronize with the Sanctuary Application Server.

---

## Installing your Synchronization Script

---

Please follow these steps to quickly get your synchronization script installation up and running (your Novell server must be ready before proceeding):

1. Install the database server. This is the first component to install since Sanctuary solution uses this database to store diverse information. The database is stored in a SQL server (full-blown version or SQL Server 2005 Express Edition SP2, depending on your company’s size). To install the database, see [Chapter 2, “Installing the Sanctuary Database”](#) on page 17.
2. Install the Sanctuary Application Server. This provides the interface between the database and the client component and between the console — used to define/modify/delete/create permissions and rules — and the database. You need to install at least one Sanctuary Application Server. This can be on the same computer as the database. To install the Sanctuary Application Server, see [Chapter 4, “Installing the Sanctuary Application Server”](#) on page 33.
3. Install the Sanctuary Management Console, to manage the definition, modification, deletion, and creation of permissions and rules. You can install the console in the same machine as the database and Sanctuary Application Server or in a different one. To install the console, see [Chapter 5, “Installing the Sanctuary Management Console”](#) on page 53.



4. Install a Novell client and our synchronization script on one of your Windows client machines. This machine must already have Novell's NDAP ActiveX objects installed (available on Novell's Web site or your installation CD). You can find the necessary synchronization script (NDSSync.vbs) in the Scripts directory.



**Note:** Windows' Gateway Services for Netware (GSNW) is not sufficient to run the NDSSync.vbs synchronization script.

5. Define simple permissions rules for the well-known accounts (Everyone, LocalSystem, etc.) using the Console installed in step 3. See the *Quick Setup Guide*.
6. Install or deploy the clients through your network to start the protection process. To install a single client, run setup.exe located in the \CLIENT folder of your installation CD: to deploy several of them, consult [Chapter 6, "Installing the Sanctuary Client on Your Endpoint Computers"](#) on page 61 and [Chapter 8, "Unattended Client Installation"](#) on page 93.



**Note:** If you are installing/uninstalling the Sanctuary Client on a Vista machine with Vista's UAC functionality turned on, you must use setup.exe (not Control Panel à Add/Remove Programs) otherwise the operation will fail.

7. Ensure that the clients are communicating with the Sanctuary Application Server and the policies defined in step 5 are enforced.
8. Run the script (c:\>cscript.exe \path\_to\_folder\NDSSync.vbs Novell\_Server\_Tree) as an Administrator on the client machine installed in step 6. You can optionally add the SQL server parameters to the script: c:\>cscript.exe \path\_to\_folder\NDSSync.vbs Novell\_Server\_Tree [<SQL Server> [<SQL User Name> <SQL Password>]. You can run this script manually from time to time (if there are not too many changes in your eDirectory structure) or automatically using a scheduler software application. See an example in [Chapter 9, "Scheduling Domain Synchronizations"](#) on page 135.

**Note:** If you are using Microsoft SQL 2005 SP1 you should specify the SQL server (optionally the user name and password), even if it is local to the machine, as (local)\SQLEXPRESS:

```
c:\>cscript.exe \path_to_folder\NDSSync.vbs Novell_Server_Tree (local)\SQLEXPRESS
```

9. When the script finishes, open the Sanctuary Management Console. You can now select the user accounts, groups, workstations, and OUs when defining permissions. Create a simple permissions rule for a device/application. Send the updates to the client machines.



**10. Test the enforcement of the new permissions rule defined in the previous step.**

**Note:** If you use NDSSync.vbs script to connect to Sanctuary Database from a remote computer, SQL Authentication is used. This is also the case when the database and console are installed on the same machine and you login as a different user. If you installed SQL 2005 Server Express Edition with our installation wizard, or manually using the Windows Authentication mode, the login options of the script cannot be used. In this case, it is impossible to synchronize Novell's eDirectory using user credentials different from those of the system administrator of the Database Server machine as NDSSync.vbs script parameters.

The following table summarizes the previous steps:

**Table F.2** Novell quick guide installation steps

Step	Description	Purpose	Reference
1	Install the database.	Store permissions, rules, and settings.	<a href="#">Chapter 2, "Installing the Sanctuary Database"</a>
2	Install the Sanctuary Application Server.	Interface between database and clients/console.	<a href="#">Chapter 4, "Installing the Sanctuary Application Server"</a>
3	Install the console.	Manage permissions, options, and rules.	<a href="#">Chapter 5, "Installing the Sanctuary Management Console"</a>
4	Install Sanctuary Synchronization script, a Novell client, and NDAP on a Windows machine.	Setup required to run Sanctuary Synchronization script.	Help file, User's Guides, <a href="#">"Script Examples"</a> , and Novell's guides
5	Define basic permissions.	Be sure that everything is working correctly by defining some permissions for well-know groups.	Help file, Quick Setup Guide, and the User's Guides.
6	Install clients.	Begin the protection process.	<a href="#">Chapter 6, "Installing the Sanctuary Client on Your Endpoint Computers"</a> and <a href="#">Chapter 8, "Unattended Client Installation"</a>



**Table F.2** Novell quick guide installation steps

Step	Description	Purpose	Reference
7	Run Sanctuary Synchronization script.	Convey all eDirectory information to the database.	<a href="#">"Script Examples"</a> on page 190
8	Define new permissions for a Novell user in the console.	Test.	Help file and User's Guides.
9	Proceed to define all of your company's policies.	Protect and enforce company's policies.	



# G Using Novell Shares for your DataFileDirectory

The information in this appendix is relevant to all Sanctuary products. If you are using Sanctuary Application Control Server Edition, be aware that this client cannot be installed on Windows XP, Windows 2000 Pro, or Windows Vista, you will be limited to an installation on Windows Server 2003.

## DataFileDirectory Access to a Novell Share

---

When installing the Sanctuary Application Server, the setup asks for a data file directory where all logs files are stored. All servers can optionally write to the same, shared, directory or you can opt for having different ones for each server (see [Figure 1.1](#), on page 2 ). It is possible to define such directory on a Novell server in the same way as it is done for a Windows server. To do this, Sanctuary Application Server must meet two conditions:

- They must be able to have create/read/write/erase access on the Novell share.
- They should have a transparent authentication access to the Novell server.

In this appendix, we explain how to create this shared directory to use transparently in a Novell environment.

## Transparent Sanctuary Application Server authentication for Novell eDirectory

---

Due to the interaction between Novell eDirectory and Microsoft Windows (Active Directory or domain environment is not required in this case), it is possible to have a transparent authentication for the Sanctuary Application Server.

Window's user credentials (name and password) are, by default, passed to Novell. If the same username (including the same password) exists in Novell, this authentication process is transparent. If this is not the case, Novell rejects the user for all non-interactive processes. If the process is an interactive one, Novell will ask for a new authentication through the Novell Client for Windows.

In essence, the process consists in setting an account in Novell's eDirectory structure with the same name and password as in Windows (local or domain user). This account is going to be used by the Sanctuary Application Server service.

We make these assumptions in the following procedure (which, of course, differs from your actual Novell installation):

- The Novell Server is called 'BOOGIE'.
- The Novell Tree is called 'Lumension'.
- The Novell Context is called 'TEST'.



- The Novell shared directory which will be used as DataFileDirectory for Sanctuary is called 'BOOGIE\_MYDATA.TEST:DataFileDir' (which is located on server BOOGIE (context TEST) hosting a shared directory (MYDATA) which contains a subdirectory named 'DataFileDir').
- The Sanctuary Application Server account used in Windows is called 'sxs'.
- The shared folder and the 'sxs' account should already exist on the Novell eDirectory. Please refer to your Novell documentation for further information about how to create shares and users in Novell. The 'sxs' account on the Novell eDirectory should have, by default, no rights to any files or directories.

Using Novell v5.0 or later, follow these steps to enable this transparent authentication:

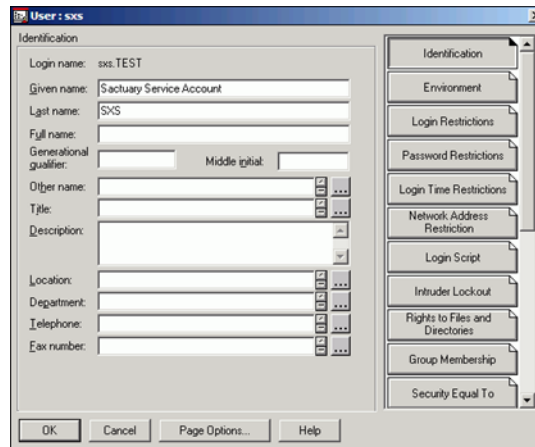
1. Run the Netware Administrator tool — nwadmn32.exe —, located at BOOGIE\SYS\PUBLIC\WIN32\ on the Novell server. This must be run from a Windows machine with a Novell Client for Windows installed on it and logged on as a Novell administrator.

Now search the user account (sxs) in the root of the context TEST. This account is used to access the Novell share by Sanctuary Application Server, as shown below:



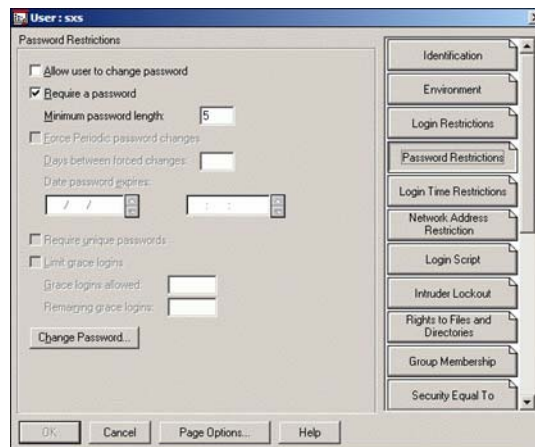
**Figure G.1** Searching the account that Sanctuary Application Server is going to use

2. Open the properties window for user 'sxs'. To do this, right click on the user and select *Details*.



**Figure G.2** Properties of the Novell account used for the Sanctuary Application Server service

3. Click *Password Restrictions* (located at the right panel of this window) and activate the *Require a password* option.



**Figure G.3** Password restrictions windows for the Novell user

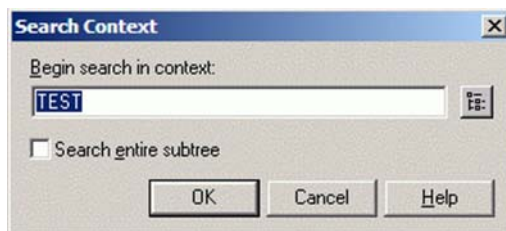


4. Click on CHANGE PASSWORD and enter the *same* password and name as for its Windows counterpart.



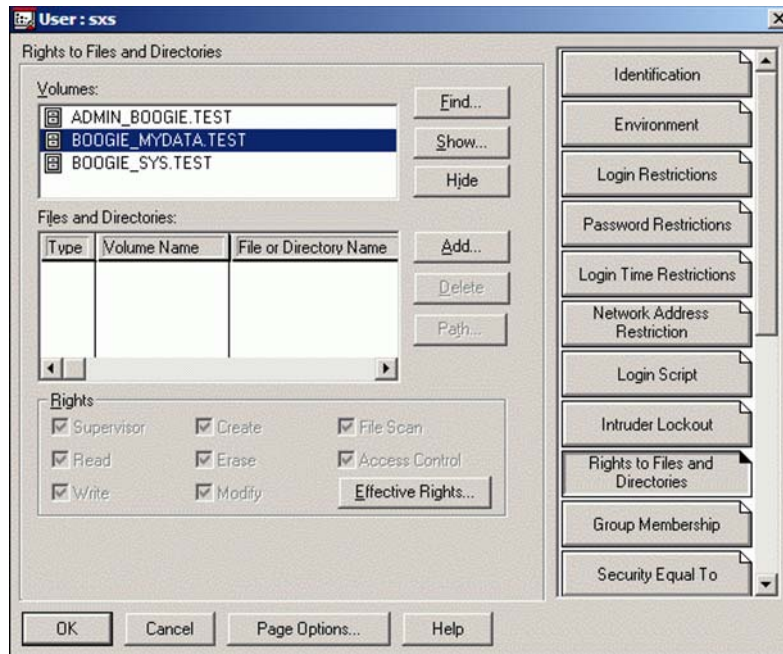
**Figure G.4** Change the password for the Novell user

5. Click on RIGHTS TO FILES AND DIRECTORIES (located on the right panel of the properties window), click on FIND, and select the TEST context:



**Figure G.5** Selecting the context for the user's rights

You should now see a window similar to the following one:



**Figure G.6** User rights for DataFileDirectory

- Click on the ADD button and traverse the tree — starting from the context TEST — until you reach the location of the data file directory object, as show in the next two screenshots.



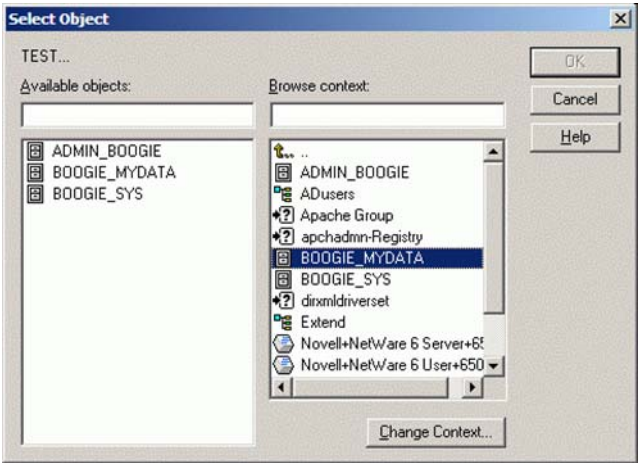


Figure G.7 Selecting the data file directory location on the Novell file server (1/2)

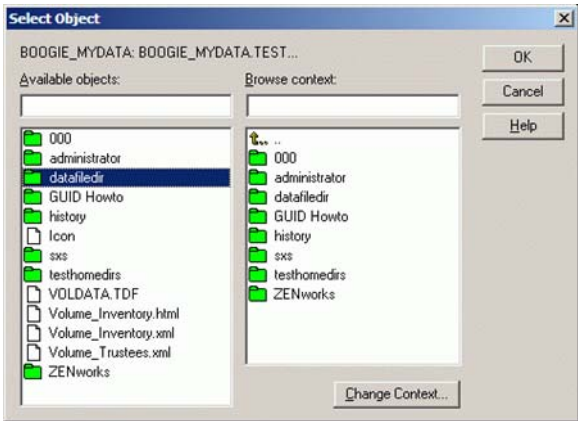


Figure G.8 Selecting the data file directory location on the Novell file server (2/2)

Once this directory is selected, give the user the following rights to it:

- READ  
Needed by Sanctuary Application Server for opening shadow files and logs.





- **WRITE**  
Required by Sanctuary Application Server to write to log files.
- **CREATE**  
Needed by Sanctuary Application Server to save fetched shadow files and create new logs.
- **ERASE**  
Required by Sanctuary Application Server when performing database maintenance.
- **MODIFY**  
Needed by Sanctuary Application Server when temporary Sanctuary Application Server files are converted into log files.
- **FILE SCAN**  
Required at startup of Sanctuary Application Server to enumerate the present shadow files and logs.





# H Installing a Certificate Authority for Encryption and TLS Communication

This appendix explains how to install and set up a Windows Certificate Authority (CA). You need a Certificate Authority to grant certificates for your clients and Sanctuary Application Server if you are going to use TLS protocol for encrypted message communication. You will also need a CA if you are planning to centrally encrypt removable devices.

## Requirements

---

You must install, publish, and properly set a Microsoft Windows Certificate Authority in order to configure a specifically managed removable media. The use of encryption to control and manage this feature fully protects against the intentional or unintentional loss of sensitive data. This section lists all mandatory requirements to install the CA needed to implement this specific product feature.



**Note:** If you are planning to install a Certificate Authority on a stand-alone server that is going to be integrated to your network later, you need to be connected to at least one computer so that Windows can recognize your network interface connector (NIC).

The Windows Certificate authority is tightly integrated to the Windows Active Directory. In order to use encryption of removable storage devices, your domain must be configured to use Active Directory.

## Integrating DNS with Active Directory

Although it is not a requirement to have the DNS integrated with Active Directory, it is important that the DNS server be properly configured.



To check if your Microsoft DNS is properly configured and integrated with Active Directory, open the DNS Management Console and check that the DNS zone contains the ‘\_msdcs’ records. The following screenshot shows how to check the DNS zone:

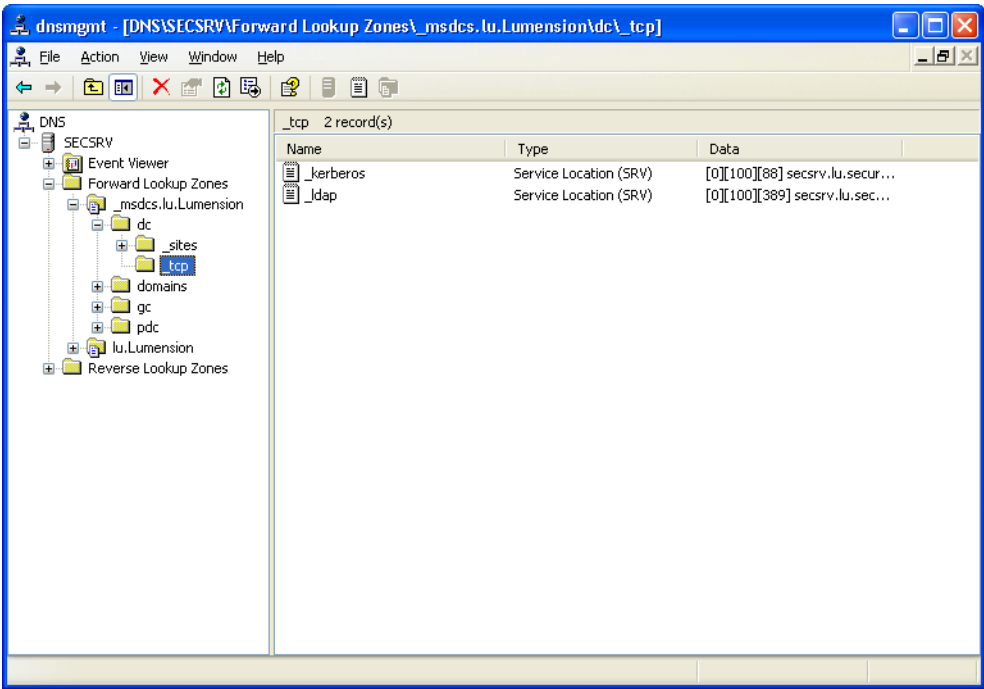


Figure H.1 Verifying the DNS zone

Please refer to the Microsoft’s Web site to get more information about how to check the configuration of your DNS servers.

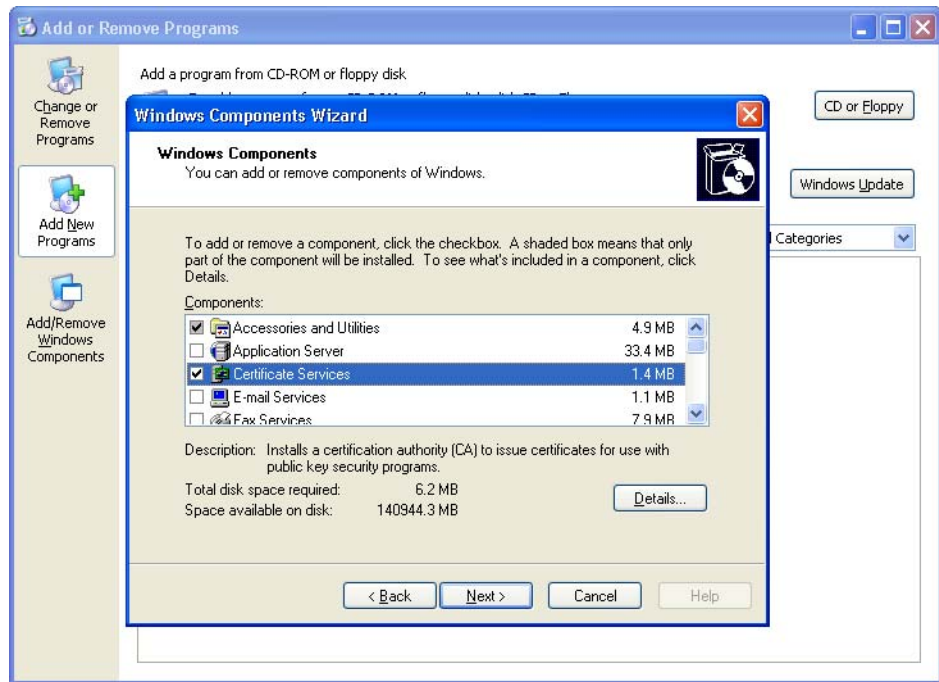
Installing the Certificate Services

If there are no certificate services installed on your network, you should follow this step-by-step procedure for the installation of the Microsoft Certificate Services.

- 1. Log on to one of the Active Directory Domain controllers as a domain administrator.
- 2. Go to the *Start → Settings → Control Panel* menu.
- 3. Click on the **ADD OR REMOVE PROGRAMS** icon.
- 4. Select **ADD/REMOVE WINDOWS COMPONENTS** located on the left part of the screen.



5. Select the *Certificate Services* entry in the list of components and click *Next*.



**Figure H.2** Adding certificate services



6. Select the *Enterprise root CA* and click *Next*.

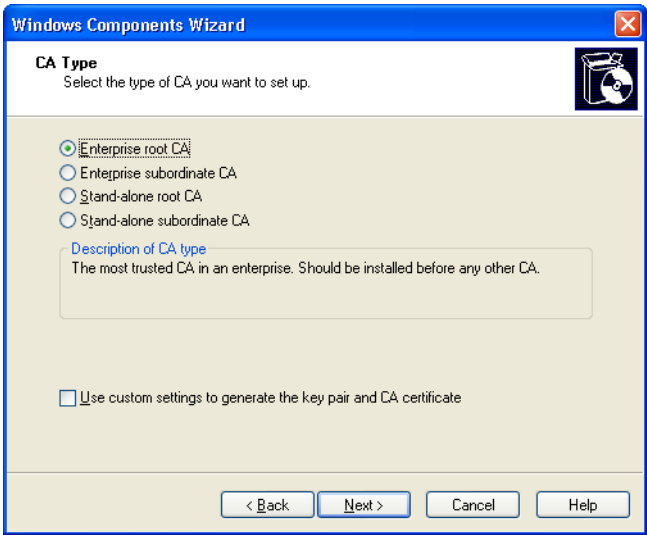
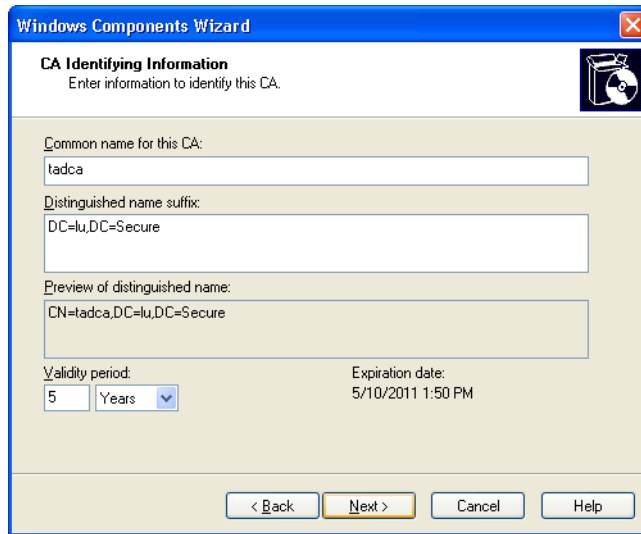


Figure H.3 The Windows components wizard (1st page)



7. Choose a *Common name* and *Distinguished name* suffix that will identify this CA and click *Next*.



The screenshot shows the 'Windows Components Wizard' window, specifically the 'CA Identifying Information' step. The window has a blue title bar and a standard Windows XP-style interface. The main area is light beige. At the top, it says 'CA Identifying Information' and 'Enter information to identify this CA.' Below this, there are three text input fields: 'Common name for this CA:' with the value 'tadca', 'Distinguished name suffix:' with the value 'DC=lu,DC=Secure', and 'Preview of distinguished name:' with the value 'CN=tadca,DC=lu,DC=Secure'. At the bottom left, there is a 'Validity period:' section with a text box containing '5' and a dropdown menu set to 'Years'. To the right of this is an 'Expiration date:' section showing '5/10/2011 1:50 PM'. At the very bottom, there are four buttons: '< Back', 'Next >', 'Cancel', and 'Help'. The 'Next >' button is highlighted with a yellow border.

**Figure H.4** The Windows components wizard (2nd page)



8. Choose an appropriate location for the Certificate Database Settings and click *Next*.

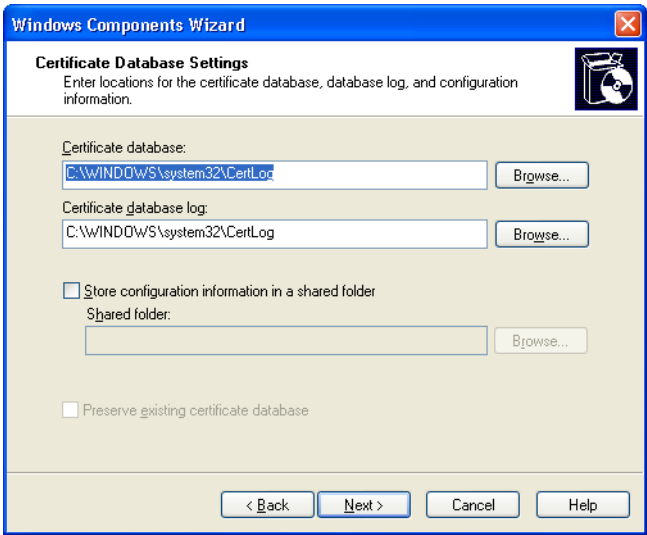
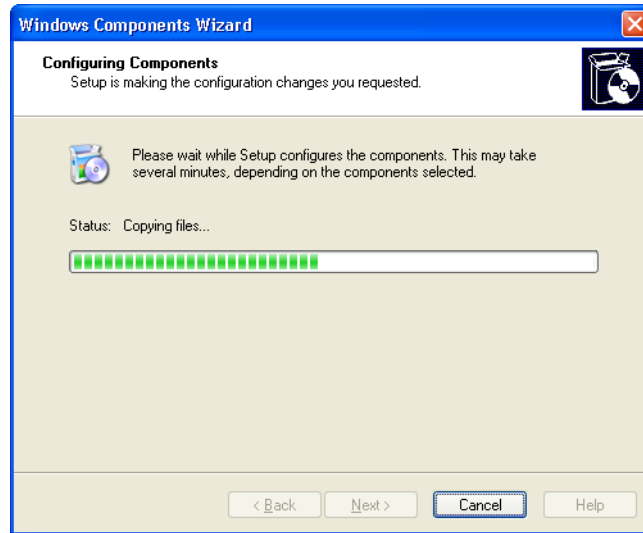


Figure H.5 The Windows components wizard (3rd page)





Windows proceeds with the certificate services installation.



**Figure H.6** The Windows components wizard (final page)



**Note:** After installation of the Sanctuary Client on the user's machine, the user must log on at least once in order to be able to access any encrypted media for which he was granted access rights. During this first logon, the user certificate is issued by the Certificate Authority. This certificate is used by the Sanctuary Application Server to deliver per-media rights for users. The Certificate is stored locally on the user's machine and additionally published to the Active Directory.



**Note:** Depending on your Active Directory configuration and replication between domain controllers setting, it may take some time to issue a certificate during the first user logon and publish it to the Active Directory. During that period, the user is not authorized to access the media.





**Note:** You must install a root enterprise level CA. There are two types of enterprise level Certificate Authority: root and subordinate. In this case, 'root and subordinate' are just Microsoft terms that identify hierarchy, thus, subordinate cannot exist without root. Since we use Active Directory (AD) integration, the CA must be able to publish and issue certificates using (AD). Only enterprise level CA is integrated with AD. The CA software of other vendors that support AD integration can also be used.

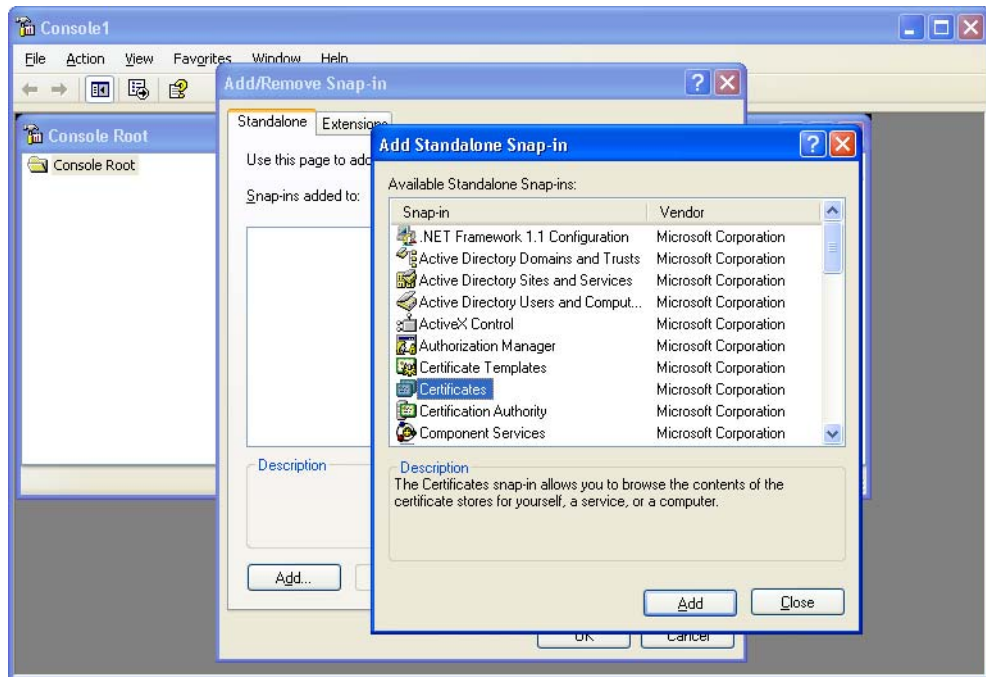
### Checking Certificates are Correctly Issued to the Users

---

If a user is denied access to an encrypted medium for which he/she has received proper rights, verify that the Certificate Authority has correctly issued the certificates for this user. The following is a step-by-step procedure to check that a user certificate has been correctly issued:

1. Log on to the user's machine.
2. Go to the *Start* → *Run* menu.
3. Enter *mmc.exe* in the *Open* field and click *OK*.
4. In the Microsoft Management console, open the *File* menu and select *Add/Remove Snap-in* (or press *Ctrl+M*).
5. Click on *ADD*.

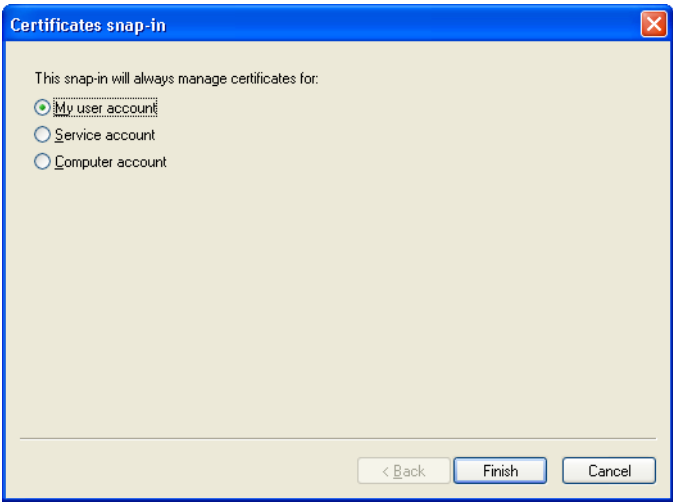
6. In the *Add Standalone Snap-in* dialog, choose *Certificates* and click *Add*.



**Figure H.7** The certificate snap-in



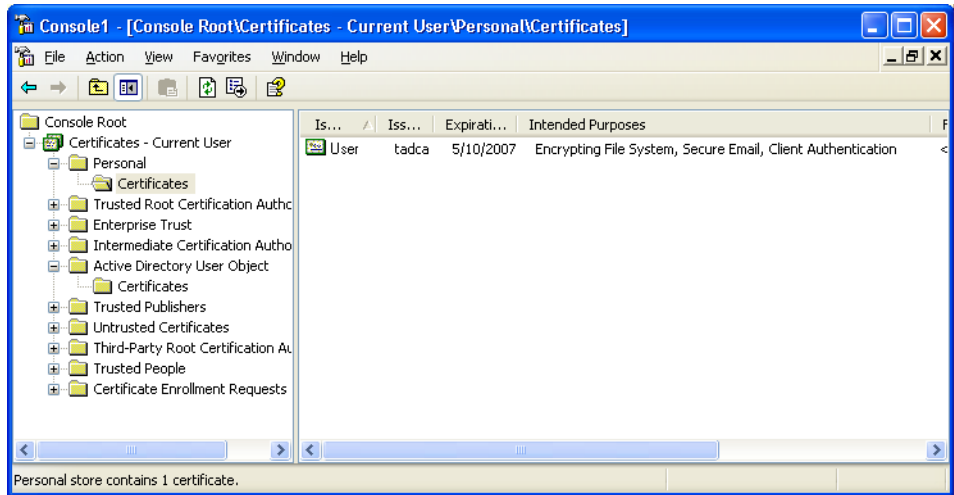
7. In the *Certificates Snap-in* dialog, choose *My user account* and click *Finish*, *Close* and *OK*.



**Figure H.8** The certificate snap-in: User account



8. Open the *Certificates – Current User* of the *Personal* node. You should see at least one entry with the *Encrypting File System, Secure Email, Client Authentication* setting in the *Intended purposes* column.



**Figure H.9** The console: Certificate intended purposes



9. Check that the same certificate entry is present under the *Certificates – Current User* node of the *Active Directory User Object*.

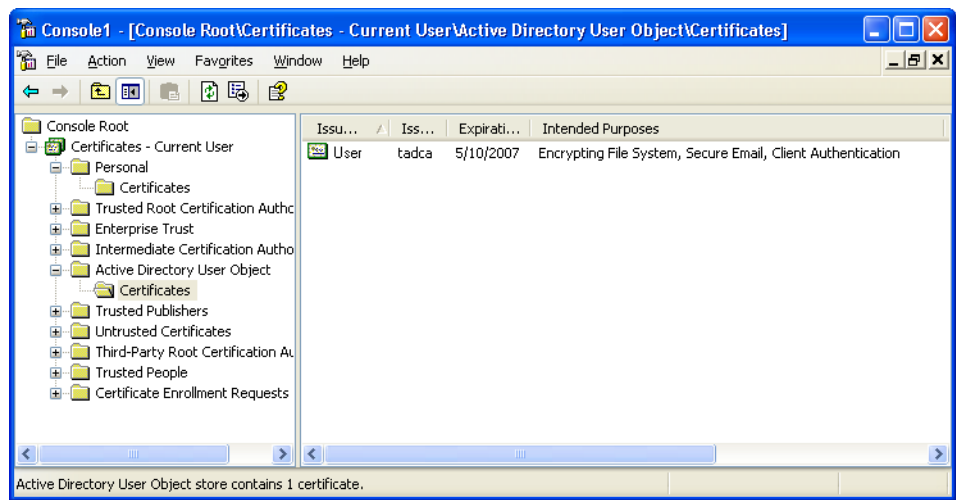


Figure H.10 Verifying the user's certificate

If the certificates are correctly issued and present on the user’s machine as described above, this user will be able to access any authorized media for which he has received appropriate permissions.



**Note:** The access permissions to encrypted removable media are retrieved from the Sanctuary Application Server by the client following any of these events:  
The user inserts and accesses an encrypted media.  
The user inserts the encrypted media and then logs on.  
It is mandatory that the Sanctuary Application Server be online and accessible upon these events. The received rights and disk encryption keys are cached locally in a protected area of the hard drive, so that the user will be able to access the encrypted media when his computer is disconnected from the network.

Checking Certificates are Correctly Issued to Endpoint Machines

If you choose to use TLS for Sanctuary Client-Sanctuary Application Server or intra-Sanctuary Application Server communications, there should exist issued certificates for each machine that uses this mode. You can verify if they were correctly emitted by using the procedure described in the “[Checking Certificates are Correctly Issued to the Users](#)” on page 210. Note that you should select *Computer Account* instead of *My user account* in step 7.



# Controlling Administrative Rights for Sanctuary's Administrators

When installing your Lumension solution, several Visual Basic Script file tools are provided. These include `Ctrlacx.vbs`, which narrows the administrative rights to control organizational units/users/computers/groups for special users designated as Sanctuary's administrators.

## Ctrlacx.vbs

`Ctrlacx.vbs` is a Visual Basic Script file that can be used to set, view, or modify the *Manage Sanctuary Settings* control rights in the Active Directory. It allows Active Directory administrators to delegate Sanctuary management for computers, users, groups, and organizational units without entrusting any other tasks (which is required by default) to them. This script may also be use to show the other control/rights defined in the Active Directory forest.

You can find `Ctrlacx.vbs` in the installation folder, usually under the `SCRIPTS` directory. You can also locate it on your installation CD.

When `Ctrlacx.vbs` runs, it creates a special entry in the permissions list of the organization unit called *Manage Sanctuary Settings*. This entry only affects Sanctuary Device Control software administrator users and the devices they control. If you assign this setting to a specific user, who is also a Sanctuary Administrator (as defined on the *User Access Manager* dialog of the console), he would only be able to manage the designated users/groups/computers for which he has rights directly from the Sanctuary Management Console.

You must synchronize with the domain after running `Ctrlacx.vbs` before these rights are activated. To do this, use the *Synchronize Domain Members* item of the *Tools* menu (or from the *Control Panel*).



**Note:** This tools does not modify the Active Directory Schema.



**Note:** You can only use this tool to create authorizations per forest, not per domain and only those users assigned as Enterprise Administrators are allowed to create, set or view control rights.

## Requirements

You must have the *Windows Script Host* (WSH, which includes `wscript.exe` and `cscript.exe`) interpreter installed on your system before you can run any VBScript. Some antivirus programs reject the execution of these types of scripts.



### Usage

To use ctrlacx.vbs:

- Open a command screen (*Start → Run → Command*) to run the script.
- Execute the script directly from the *Run* dialog

In both cases use the following syntax:

```
cscript Ctrlacx.vbs [-parameter list]>file.txt
```

where the parameters are explained in the following list.

The previous syntax sends the output directly to a text file specified, in this case, by *file.txt*. If you want to use it interactively, utilize the following syntax:

```
ctrlacx.vbs [-parameter list]
```

- or -

```
wscript Ctrlacx.vbs [-parameter list]
```

You can use the following parameters for the Ctrlacx script:

- -?  
Displays a brief description of each possible parameter. You must run this script in interactive mode or from the command line in order to see the text.
- -e  
Enumerate all control access rights. Condensed output.
- -v  
Enumerate all control access rights. Detailed output (verbose).
- -q cn  
Displays a control right by its canonical name (cn).
- -s  
Display Lumension's Manage Sanctuary Settings rights.
- -create  
Creates or updates Lumension's Manage Sanctuary Settings rights.
- -delete  
Deletes Lumension's Manage Sanctuary Settings rights.

### Examples

To list all control access rights in condensed mode redirecting the output to MyFile.txt file.

```
cscript Ctrlacx.vbs -e > MyFile.txt
```

To show the *Manage Sanctuary Settings* rights interactively.

```
ctrlacx.vbs -s
```

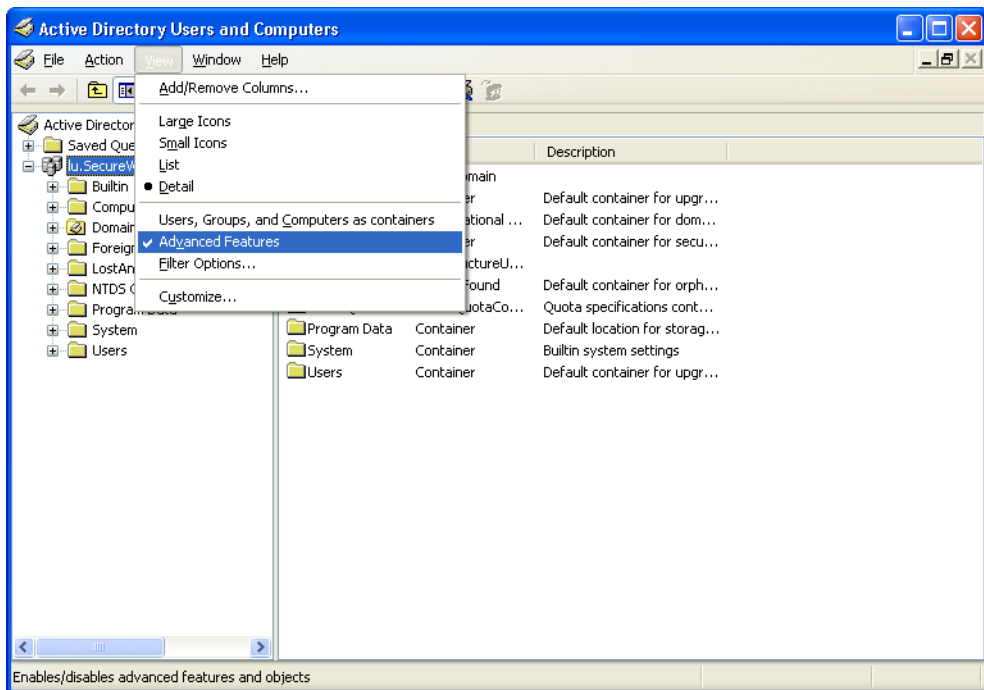




## What to do After Running the Script

Once you run the script on a domain machine, you have to assign the delegation rights you just created for Sanctuary. To do this, follow these steps:

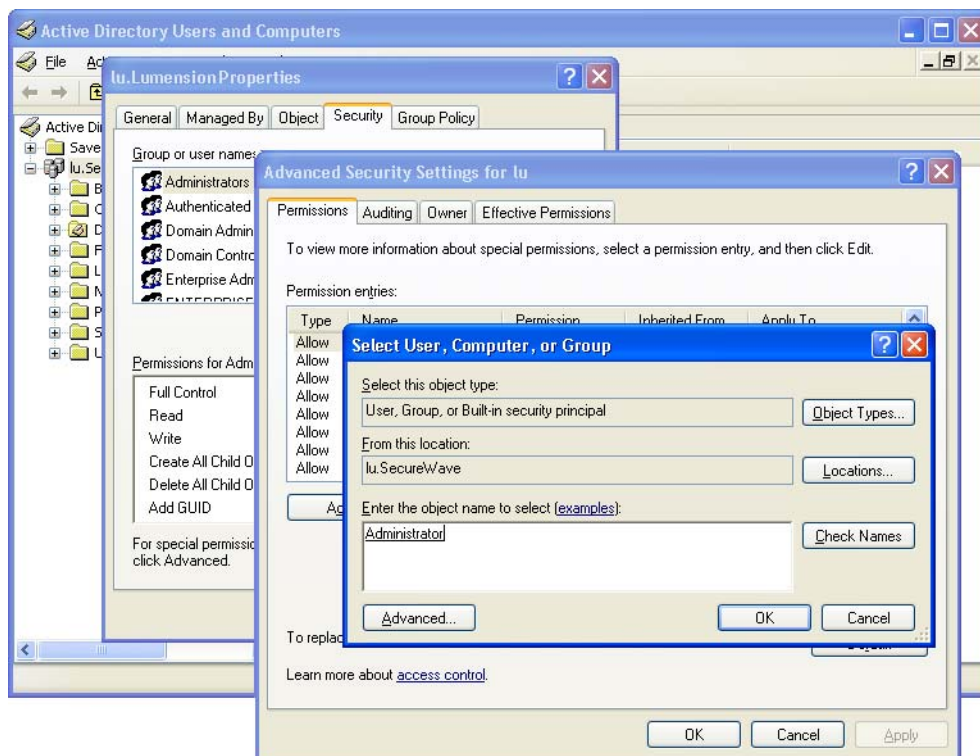
1. Run the script with the *-create* parameter to generate or update Lumension's rights on the active directory.
2. Open the Microsoft Management Console (MMC) window.
3. Activate the *Advanced Features* option from the *View* menu:



**Figure I.1** Advanced feature option of the MMC

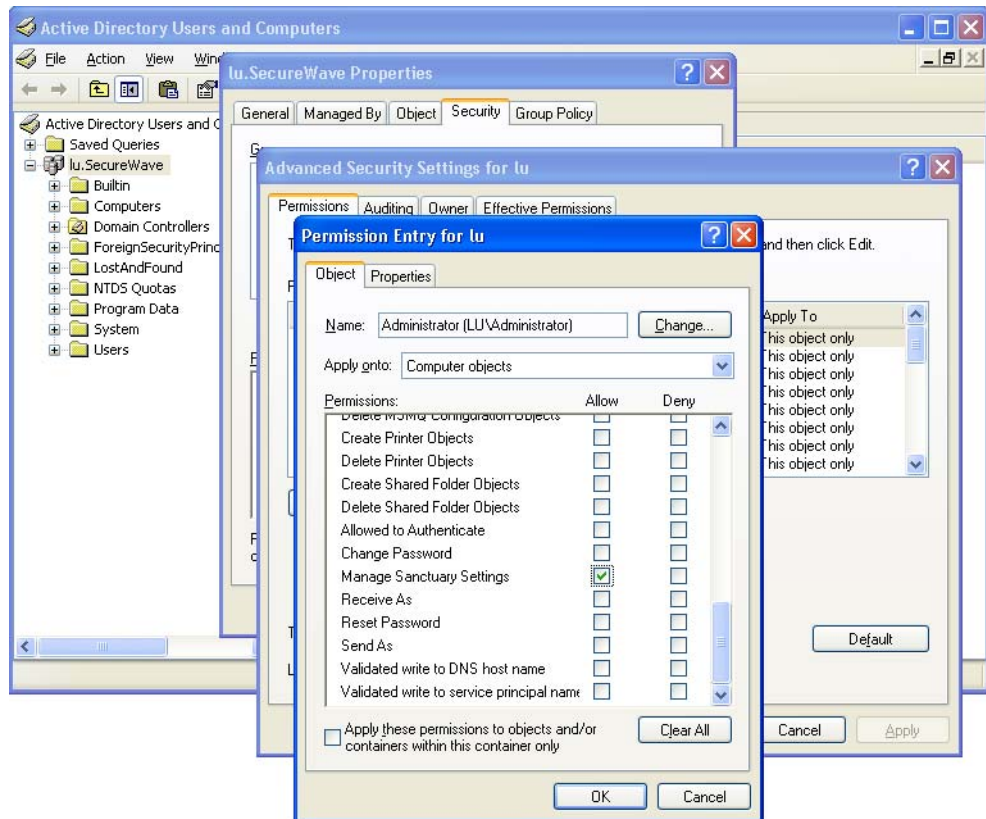
4. Right click on the desired Organizational Unit (OU) and select *Properties* from the pop-up menu.
5. Go to the *Security* tab and click on *ADVANCED* to open the *Advanced Security Settings* dialog.
6. Go to the *Permissions* tab and click on *ADD* or *EDIT*.
7. Select the user or group to which you want to delegate rights, as shown in the following image.





**Figure I.2** Select user, computer, or group to which delegate

8. Click on OBJECT TYPES, select *Computers* and click on OK to close the dialog
9. Click on the OK button to open the *Permissions entry* dialog:



**Figure I.3** Manage Sanctuary Settings object

Three important objects exist in the *Apply onto* field of this dialog that are relevant to the Sanctuary settings: *Computer objects*, *Group objects*, and *User objects*. Figure 3 shows only one of them: *Computer objects*.

The script narrows the Active Directory rights by creating a special entry in each of the above-mentioned objects: *Manage Sanctuary Settings*. If you assign this permission to a user, he/she can only manage the designated users/groups/computers in the Sanctuary Management Console.

Note the special check box option in the permissions entry: *Apply these permissions to objects and/or containers within this container only*. If activated, you will see only the real objects — users or computers from this OU — in the console and nothing from the child OUs beneath.

The ‘new’ delegated administrator can now manage the objects (users/computers/groups) explicitly assigned to him.





# J Installation Checklist

## Requirements

---

Before starting to install any Sanctuary products make sure to have the following:

### If you are Using Windows...

- Active Directory installed and configured within a domain.
- Configure DNS as AD integrated and create a reverse lookup zone
- or –
- A workgroup network properly configured.

### If you are Using Novell...

- NDAP installed on the machine you are going to use to synchronize your eDirectory structure. We recommend installing it on the same machine as the database server.
- ZENworks client optionally installed on the client computer.

## The Sanctuary Database

The database is used to hold permissions, logs, available in-line machines, users, devices, etc. There is only one database per organization but you can use SQL clustering for disaster recovery purposes.

### Software

The Database component requires a Microsoft SQL Server database. This can either be Microsoft SQL Server 2000 SP4/2005 SP2/2005 SP2 64-bit or Microsoft SQL Server 2005 Express Edition SP2. If you do not have an SQL server, you can install Microsoft SQL Server 2005 Express Edition directly from the Sanctuary's CD.

### Hardware

The hardware specifications of the database server should be the following, as a minimum (depending on your enterprise size and number of clients):

- Memory: 512 MB (2GB recommended).
- CPU: Pentium 3 or 4 processor or equivalent AMD processor.
- HD: 3 GB SCSI or IDE.
- NIC 100 MBits/s.



### Network Configuration

- Configure your DNS server.
- DHCP server started.

### Additional Settings

- Change the Event Viewer settings to 1024 KB in size and choose to overwrite events as needed.
- Change the Performance settings to prioritize for background applications.

### Firewall Configuration

If you are using Windows XP (SP2 or later), Windows 2003 Server (SP1 or later), or Windows Vista for the database, the firewall may be active and blocking certain ports needed to communicate with the Sanctuary Application Server.

## The Sanctuary Application Server

The Sanctuary Application Server handles client logons and is the only component that connects to the database.

### Software

- Windows 2000/2003 Server with latest service packs.
- Install Microsoft Enterprise Certificate Authority (root) for central encryption.
- A PDF Viewer to read the documents.
- MDAC v2.6 with SP1 or later if you are using Windows 2000 server

### Hardware

The hardware specifications of the Sanctuary Application Server should be the following, as a minimum (depending on your enterprise size and number of clients):

- Memory: 256 MB (512 recommended).
- CPU: Pentium 3 or 4 processor or equivalent AMD processor.
- HD: 3 GB SCSI or IDE (bigger if you plan to use shadow when installing Sanctuary Device Control and if the Data File Directory (see [“Data file directory”](#) on page 224) is defined on this machine.
- NIC 100 MBits/s.

## The Sanctuary Management Console

The Sanctuary Management Console is the application that you use to administer your Sanctuary suite. You can install it on as many computers as you want.





**Note:** You must install the client in the Sanctuary Management Console machine if you are planning to encrypt and/or authorize removable media.

## Firewall Configuration

If you are using Windows XP (SP2 or later), Windows 2003 Server (SP1 or later), or Windows Vista for the console the firewall may be active and blocking certain ports needed to communicate with the Sanctuary Application Server.

## Sanctuary Client

The Sanctuary Client is the software used to manage the devices or authorize software execution on the client(s) computer. You can install it individually in each machine to be protected or — in large organizations, or when you cannot visit each client computer (server) individually — using our unattended client installation software. You can also use any other software that supports MSI packages to install Sanctuary Clients.

## Software

If you are using Sanctuary Device Control or Sanctuary Application Control, the client requires a Windows XP SP2 (32-bit or 64-bit), Windows 2000 SP4, Windows Vista (32-bit or 64-bit) or Windows 2003 SP1 (32-bit or 64-bit) machine. We recommend defining Windows updates from Windows Server Update Services (WSUS) if you are installing Sanctuary Application Control Suite.

If you are using Sanctuary Application Control Server Edition or Sanctuary Application Control Terminal Services Edition the you should only use Windows 2000 Server (SP 4 or later) Windows Server 2003 SP1 or later.

## Hardware

The hardware specifications of the client should at least meet the following ones:

- Memory: 256 MB (512 recommended).
- CPU: Pentium 3 or 4 processor or equivalent AMD processor.
- HD (SCSI or IDE): 10 Mb to install the client and several GB of free space if you are planning to activate or not the 'full shadow' feature when installing Sanctuary Device Control.
- NIC 100 MBits/s.

## Network Configuration

- Select the corresponding DNS server.
- Configure the NIC for receiving IP by the DHCP service.



### Additional Settings

- If you are using Sanctuary Client in a Novell eDirectory: Install the Novell, and optionally the ZENworks, client.
- Change the Event viewer settings to 1024 KB in size and choose to overwrite events as needed.

### Firewall Configuration

Unblock firewall ports as needed to communicate with the Sanctuary Application Server. This is particularly important if you are using Windows XP SP3 or Windows Vista.

### License

Each Sanctuary Application Server has a license file that specifies whether you have a valid copy of one or several of our Sanctuary programs, for example, Sanctuary Application Control Server Edition, Sanctuary Device Control, and so on.

There are two types of license available:

- Evaluation license.
- Full license.

When you receive the license file, copy it to the %SYSTEMROOT%\SYSTEM32 folder of each computer that runs the Sanctuary Application Server. It is *not* required on client machines.

### Private and Public Keys

Sanctuary provides a utility that you can use to create a key pair that is used to assure communication integrity between the Sanctuary Application Server and the client.

In a production environment, you must create your own key pair **before installing the** Sanctuary Application Server and deploying the first Sanctuary Client.

### Data file directory

When installing the Sanctuary Application Server, the setup asks for at least one data file directory where all shadow and log information is stored. We call it DataFileDirectory or DFD.

A permanent network share should be used when planning to use more than one Sanctuary Application Server, as all servers need to write to the **same**, shared, directory (several ones can be defined). On the other hand, for evaluation purposes a local directory is better.

It is possible to define such directory if you are using a Novell server in the same way as it is done for a Windows server. If your DFD is defined on a Novell server, you should use an account with the same name and password to access this shared directory.

You should take into consideration the hard disk drive size when defining log options.





## SXS Account

The Sanctuary Application Server service requires a user account to run. Use a domain account (any domain user, an administrative account is **not** required) if you plan to use your Sanctuary software in a domain environment. Use a local account if you plan to administer computers in a workgroup.

## Certificate Authority

You must have a Certificate Authority installed and configured if you plan to use the TLS protocol when installing the clients and/or central encryption if installing Sanctuary Device Control.

Microsoft's Certificate Authority installation is described in [Appendix H, "Installing a Certificate Authority for Encryption and TLS Communication"](#) on page 203.

## Implementation Actions

To help you to implement Sanctuary, the following table explains the actions required:

**Table J.1** Implementation actions

#	Action	Description
1	Create devices, media, and software inventory. We provide a special software tool for you device inventory, Sanctuary Device Scanner Tool, in our Web site.	The inventory lists all devices and media that you want to control (depending on which Sanctuary products you bought).
2	Write a company policy that defines the permissions, shadowing options, encrypted devices, Sanctuary administrators/roles, and Add Domain Global Groups for Sanctuary permissions and Sanctuary administrators (optional).	The document of the company's policies lists all the settings that are used to control Sanctuary's installation. It includes permissions and to whom they will be assigned, users that will become Sanctuary Administrators, etc.
3	Plan the architecture of the installation, based on the sizing considerations.	The resulting document can be a network diagram that reflects the architecture together with server's hostnames and IP addresses.
4	Create a Sanctuary Application Server service account in your Domain.	The Sanctuary Application Server is a standard Windows service that runs under a regular account. It is a good practice to create a new dedicated, domain account, for this purpose and set its options to 'User cannot change password' and 'Password never expires'. This account <b>MUST</b> have local administration rights if you plan to use TLS for client-Sanctuary Application Server or intra-Sanctuary Application Server communications.



**Table J.1** Implementation actions

#	Action	Description
5	Install a Microsoft Enterprise Certificate Authority for Encryption or TLS protocol for client – Sanctuary Application Server or intra-Sanctuary Application Server communications.	In case you want to encrypt removable devices such as pen drives, memory sticks, and so on, we recommend you install a Microsoft Enterprise Certificate Authority. You also need this component if you plan to use TLS protocol for Sanctuary Client–Sanctuary Application Server or intra–Sanctuary Application Server communications (all messages are encrypted). If you do not use TLS protocol, all messages are signed using the private key.
6	Install DBMS: MSSQL 2000 SP4/2005 SP2/ 2005 SP2 64 bits or MSSQL 2005 Express Edition SP2.	The Database Management System used by Sanctuary is either a Microsoft SQL Server 2000 SP4/2005 SP2/ 2005 64 bits or Microsoft SQL 2005 Express Edition SP2 — depending on the number of clients to be controlled.
7	Install Sanctuary Database and grant owner rights to the Sanctuary Application Server service account.	The Sanctuary Database is installed and you grant owner rights to the Sanctuary Application Server Service account, before starting the installation of the first Sanctuary Application Server.
8	Create a Share (DataFileDirectory) for the Sanctuary Application Server on a fileserver (required in configurations with multiple Sanctuary Application Servers).	If the sizing analysis has determined that more than one Sanctuary Application Server should be used, you must create a network share (DataFileDirectory - a common repository to all Sanctuary Application Server) before installing the first Sanctuary Application Server. If you are going to use only one Sanctuary Application Server, this can be local to the machine where the Sanctuary Application Server is going to be installed.
9	Generate a new key-pair to secure the communication between the Sanctuary Application Server and the clients.	Before the first Sanctuary Application Server is installed, create your own key-pair and implement this key-pair where the first Sanctuary Application Server will be installed (copy both keys to the '%SystemRoot%\SxsData' folder).
10	Install the first Sanctuary Application Server.	Install the first Sanctuary Application Server, taking into account the following: Use the Sanctuary Application Server service account. Connect to the DBMS that hosts the Sanctuary Database. Use the defined Network Share for the DataFileDirectory.
11	Install additional Sanctuary Application Servers and licenses.	If more Sanctuary Application Servers are needed, you can proceed to install them following the same steps as for the first Sanctuary Application Server. You need a license for each installation. After each installation, copy your own key-pair, so that all Sanctuary Application Server are using the same ones.



**Table J.1** Implementation actions

#	Action	Description
12	Install the Sanctuary Management Console.	Install the console on the selected machines. Also, install the client on the same machine(s) if you are using Sanctuary Device Control and you are planning to centrally encrypt devices and authorize media.
13	Schedule Domain (and Novell's objects) synchronization.	Schedule a task with the command-line tool 'sxdomain.exe' that will synchronize all relevant objects from your domain into Sanctuary Database. Create another task if you are working on a Novell environment (NDSSync.vbs).
14	Add devices and media from your inventory into the Sanctuary Database (if needed/ wanted) in order to assign permissions.	If you have planned to assign permissions for specific models or uniquely identified media (CD/DVD or Removable devices), add them to the database.
15	Assign permissions and options based on the company policy and Devices/Applications inventory and define the Sanctuary Administrators.	Assign the permissions for the devices, media, and software to the domain groups. Also, define the Sanctuary Administrators.
16	Install a Sanctuary Client on a test workstation.	Install the client software on a test workstation and connect it to the server components.
17	Validate the test client installation and permissions.	Test your installation on functionality, validate the permissions defined in the previous step. If necessary, adapt the permissions and update the Company Policy.
18	Prepare and test the Sanctuary Client Deployment Tool package.	Prepare the deploy package of the Sanctuary Client software based on the instructions of this Sanctuary Setup Guide and your existing, internal procedures. Check the public key file, policies exportation data, and MST Installer Transform file.
19	Deploy the client software.	Deploy Sanctuary Client to all client computers. Read the notes regarding policy exportation.

## Installation checklist

The following table guides you through the steps needed to install the Sanctuary solution from A to Z:



**Table J.2** Installation checklist

#	Description	Done/ Resolved	Comments	Reference
1	Verify the minimum requirements for each component.	<input type="checkbox"/>	-	<a href="#">Appendix A, "Detailed System Requirements and Limitations"</a>
2	Are you using a firewall or are you installing the Console on Windows XP SP3/ Windows Vista with the firewall activated?	<input type="checkbox"/>	Open needed ports. Seal/chassis intrusion protector, Password protected BIOS, NTFS Partition, etc.	<a href="#">Appendix E, "Opening Firewall Ports for Client Deployment"</a>
3	Do all basic protection steps for all your computers?	<input type="checkbox"/>	Only recommended when testing the product.	See the Sanctuary Quick Setup Guide
4	Decide between using a full-blown SQL Server or the 'light' version.	<input type="checkbox"/>	Install the SQL Server 2005 Express Edition or use your SQL Server.	<a href="#">"Choosing a SQL Engine"</a> on page 17
5	Are you installing the Sanctuary Database, Sanctuary Application Server, and Sanctuary Management Console in the same physical machine?	<input type="checkbox"/>	Create the 'sx' database.	This is done automatically by installing the database (see next step)
6	Install the Sanctuary Database.	<input type="checkbox"/>	Install MDAC 2.6 SP1 (already installed with SQL 2000 SP4).	<a href="#">"Stage 1: To Install the SQL Database Engine"</a> on page 19
		<input type="checkbox"/>	Create the 'sx' database	<a href="#">"Stage 2: To Install the Sanctuary Database "</a> on page 20



**Table J.2** Installation checklist

#	Description	Done/ Resolved	Comments	Reference
7	Install Sanctuary Application Server. (Are you going to have a single Sanctuary Application Server?)	<input type="checkbox"/>	Install MDAC 2.6 SP1 (already installed with SQL 2000 SP4)	Microsoft's Web site
		<input type="checkbox"/>	If doing central encryption or using TLS for your clients, install a Certification Authority.	See Sanctuary Device Control User Guide
		<input type="checkbox"/>	Define a fixed IP for his machine.	Configure DHCP / DNS correctly. Windows' manuals or help file, see <a href="#">"Before you Install"</a> on page 18
		<input type="checkbox"/>	If installing on a different machine from that of the database, check that the Sanctuary Application Server has the proper rights to use the database.	See <a href="#">"Before you Install"</a> on page 18
		<input type="checkbox"/>	Check license file.	See <a href="#">"Before you Install"</a> on page 18
		<input type="checkbox"/>	Generate key pair to encrypt communication between server(s) and clients (only once).	<a href="#">Chapter 3, "Using the Key Pair Generator"</a>
8	Are you going to have a single Sanctuary Management Console?	<input type="checkbox"/>	Install the Sanctuary Management Console	<a href="#">Chapter 5, "Installing the Sanctuary Management Console"</a>
		<input type="checkbox"/>	Synchronize domain members to fill-up the database.	<a href="#">Chapter 9, "Using the SXDomain Command Line Tool"</a>
9	Are you planning to centrally encrypt media? (if using Sanctuary Device Control)	<input type="checkbox"/>	Install client on Console machine.	<a href="#">Chapter 6, "Installing the Sanctuary Client on Your Endpoint Computers"</a>
		<input type="checkbox"/>	Install Microsoft Enterprise Certificate Authority (optionally) on a Domain Controller.	See Sanctuary Device Control User Guide. Microsoft's Web site.
10	Are you using TLS for your clients or intra-Sanctuary Application Server communications?	<input type="checkbox"/>	Install Microsoft Enterprise Certificate Authority on a Domain Controller.	See Sanctuary Device Control User Guide. Microsoft's Web site.
11	Install a single client machine for testing purposes.	<input type="checkbox"/>	Better to do this on a test machine that you can fully control.	See the Sanctuary Quick Setup Guide.



**Table J.2** Installation checklist

#	Description	Done/ Resolved	Comments		Reference
12	Test your installation.	<input type="checkbox"/>	Test device/application denial when accessing a device (e.g. CD drive).		Consult the Sanctuary Quick Setup Guide.
		<input type="checkbox"/>	Define simple permissions for a device/application (e.g. CD drive or Calculator).		
		<input type="checkbox"/>	Re-test for the permission defined in previous step.		
		<input type="checkbox"/>	Check different permissions and options to understand how the program works.		
13	Deploy clients.	<input type="checkbox"/>	Create MSI installation packages using public key generated on step 7.		<a href="#">"To Install Packages"</a> on page 97
		<input type="checkbox"/>	Do you already have permission definitions from a subsidiary/previous Sanctuary installation? Optionally create policies.dat		Consult the Users' Guides
		<input type="checkbox"/>	Assign computers to the installation package(s).		<a href="#">Chapter 8, "Unattended Client Installation"</a>
		Deploy	<input type="checkbox"/>	Automatically	<a href="#">Chapter 8, "Unattended Client Installation"</a>
			<input type="checkbox"/>	Command line	<a href="#">"Using the Command Line to Install Clients"</a> on page 117
			<input type="checkbox"/>	Windows' group policy	<a href="#">"Using Windows Group Policy to Install Clients"</a> on page 118
14	Schedule the domain synchronization process.	<input type="checkbox"/>	-		<a href="#">"Scheduling Domain Synchronizations"</a> on page 135
15	Are you using Novell machines?	<input type="checkbox"/>	Synchronize eDirectory objects		<a href="#">Appendix F, "Using the Synchronization Script for Novell"</a>
16	Define permissions, rules, and options according to corporate policies.	<input type="checkbox"/>	-		Consult the Users' Guides. See also next table



## Defining Permissions in Sanctuary Device Control

Use the following table as guideline when setting permissions. It defines which ones can be set depending on the group where you are working:

**Table J.3** Defining permissions

Permission type	Description																
		Biometric devices	COM/Serial ports	DVD/CD drives	Floppy disk drives	Imaging devices	LPT/Parallel ports	Modems/Secondary network access devices	Palm handheld devices	Printers (USB)	PS/2 Ports	Removable storage devices	RIM BlackBerry handhelds	Smart Card readers	Tape drives	User-defined devices	Windows CE handheld devices
Root level	Event notification																
	Permissions (R, R/W, or None)																
Device Class level	Permissions (R, R/W, or None)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Online permissions	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Offline permissions	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Scheduled permissions		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>	
	Temporary permissions																
	Shadow		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>				<input type="checkbox"/>					
	Copy Limit				<input type="checkbox"/>							<input type="checkbox"/>					
	Event notification	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Decentralized encryption											<input type="checkbox"/>					
	File type filtering			<input type="checkbox"/>	<input type="checkbox"/>							<input type="checkbox"/>					



**Table J.3** Defining permissions

Permission type	Description	Biometric devices	COM/Serial ports	DVD/CD drives	Floppy disk drives	Imaging devices	LPT/Parallel ports	Modems/Secondary network access devices	Palm handheld devices	Printers (USB)	PS/2 Ports	Removable storage devices	RIM BlackBerry handhelds	Smart Card readers	Tape drives	User-defined devices	Windows CE handheld devices	Wireless NICs (network interface controllers)
Device Group level	Permissions (R, R/W, or None)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Online permissions	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Offline permissions	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Scheduled permissions	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Temporary permissions	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Shadow	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Copy Limit	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Event notification	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Decentralized encryption	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	File type filtering	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>





**Table J.3** Defining permissions

Permission type	Description	Biometric devices	COM/Serial ports	DVD/CD drives	Floppy disk drives	Imaging devices	LPT/Parallel ports	Modems/Secondary network access devices	Palm handheld devices	Printers (USB)	PS/2 Ports	Removable storage devices	RIM BlackBerry handhelds	Smart Card readers	Tape drives	User-defined devices	Windows CE handheld devices	Wireless NICs (network interface controllers)
Device Level	Permissions (R, R/W, or None)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Online permissions	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Offline permissions	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Scheduled permissions	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Temporary permissions	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Shadow	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Copy Limit	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Event notification	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Decentralized encryption	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	File type filtering	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>



**Table J.3** Defining permissions

Permission type	Description	Biometric devices	COM/Serial ports	DVD/CD drives	Floppy disk drives	Imaging devices	LPT/Parallel ports	Modems/Secondary network access devices	Palm handheld devices	Printers (USB)	PS/2 Ports	Removable storage devices	RIM BlackBerry handhelds	Smart Card readers	Tape drives	User-defined devices	Windows CE handheld devices	Wireless NICs (network interface controllers)
Computer Level	Permissions (R, R/W, or None)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Online permissions	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Offline permissions	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Scheduled permissions	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Temporary permissions	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Shadow	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Copy Limit	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Event notification	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Decentralized encryption	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	File type filtering	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>



**Table J.3** Defining permissions

Permission type	Description	Biometric devices	COM/Serial ports	DVD/CD drives	Floppy disk drives	Imaging devices	LPT/Parallel ports	Modems/Secondary network access devices	Palm handheld devices	Printers (USB)	PS/2 Ports	Removable storage devices	RIM BlackBerry handhelds	Smart Card readers	Tape drives	User-defined devices	Windows CE handheld devices	Wireless NICs (network interface controllers)
Computer Group Level	Permissions (R, R/W, or None)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Online permissions	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Offline permissions	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Scheduled permissions		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
	Temporary permissions		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>						
	Shadow		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>				<input type="checkbox"/>						
	Copy Limit				<input type="checkbox"/>							<input type="checkbox"/>						
	Event notification	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Decentralized encryption											<input type="checkbox"/>						
	File type filtering			<input type="checkbox"/>	<input type="checkbox"/>							<input type="checkbox"/>						



**Table J.3** Defining permissions

Permission type	Description	Biometric devices	COM/Serial ports	DVD/CD drives	Floppy disk drives	Imaging devices	LPT/Parallel ports	Modems/Secondary network access devices	Palm handheld devices	Printers (USB)	PS/2 Ports	Removable storage devices	RIM BlackBerry handhelds	Smart Card readers	Tape drives	User-defined devices	Windows CE handheld devices	Wireless NICs (network interface controllers)
Group Settings	Permissions (R, R/W, or None)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Online permissions	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Offline permissions	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Scheduled permissions	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Temporary permissions	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Shadow	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Copy Limit	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Event notification	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Specific Setting	Permissions (R, R/W, or None)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Online permissions	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Offline permissions	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Scheduled permissions	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Temporary permissions	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Shadow	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Copy Limit	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Event notification	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>



# K Installing Sanctuary Application Control Terminal Services Edition

## Introducing Sanctuary Application Control Terminal Services Edition

---

Sanctuary Application Control Terminal Services Edition is a proactive software security solution that gives you the ability to exercise total control over applications' execution on your Citrix MetaFrame Presentation Servers. Sanctuary Application Control Terminal Services Edition works on the basis that unless an executable is explicitly authorized, its execution is denied.

Using Sanctuary Application Control Terminal Services Edition ensures that:

- Your users cannot execute programs such as hacking tools, games, or unlicensed software.
- You eliminate the threats posed by Trojans, Worms, and executable viruses, both known and unknown.

Sanctuary Application Control Terminal Services Edition works exactly the opposite way to most security and anti-virus products on the market: Rather than creating a 'black list' of files that are not allowed to run, Sanctuary Application Control Terminal Services Edition uses a 'white list' of executable files that are allowed to run. This is done by identifying these allowed files and creating their digital digest (hash) which is then stored in the central database. These hashes are associated with File Groups that are, in turn, associated with users/user groups that are allowed to run them.

This innovative approach offers several significant benefits:

- Greater protection. It does not matter that new Trojans and viruses are written since you purchased Sanctuary Application Control Terminal Services Edition. Any unknown or unauthorized executable, regardless of its origin, simply will not run.
- There is no requirement for regular updates for every new virus, as there is no 'black list' to maintain.
- Requests for execution are intercepted before an executable file is allowed to run, preventing execution altogether.
- You do not need to know precisely which software is installed on every MetaFrame Presentation Server on your LAN or WAN.
- It does not matter how the unauthorized application entered the MetaFrame Presentation Server, (through email, Internet, or network share) Sanctuary Application Control Terminal Services Edition will stop it from being executed.

## Installing the Server Side Components

---

Given Sanctuary Application Control Terminal Services Edition three-tier architecture, you need first to install Sanctuary's server side components. The exact procedure has already been described in the first chapters of this guide.



The server and administrative components should be installed onto *another* server — not the one you wish to control. For evaluation purposes, any workstation or server will do as long as the Terminal Services or MetaFrame Presentation Server is not installed.

Once installed, you can take advantage of the Standard File Definitions (SFD) to populate the Sanctuary Database with file signatures for your operating system. If not done during the installation, you can proceed to the Sanctuary Management Console, and select *Tools* → *Import Standard File Definitions* from the menu. In the dialog that is displayed, begin by selecting the lists to be imported (click the *Add* button); you will find them in the \SFD folder on the Sanctuary Application Control Terminal Services Edition CD-ROM. Click the *Import* button to start the process.

Once the file definitions importation finishes, you should select the *User Explorer* module (from the same console) and assign the newly created File Groups to users as follows:

- Everyone: Windows Common, Logon Files
- LocalSystem : Boot Files
- LOCAL SERVICE: Boot Files
- NETWORK SERVICE: Boot Files
- Administrators: all

These assignments represent the minimum that we recommend. Additionally, you may want to assign Entertainment, Communication, Accessories, Control Panel, DOS Applications, and 16bit Applications to users or groups as required.

All other files can be authorized either by means of the execution logs (*Log Explorer* module) or by scanning the target computer (*Scan Explorer* module). Please refer to the *Sanctuary Application Control Suite User Guide* for further details.

## Installing the Sanctuary Client

---

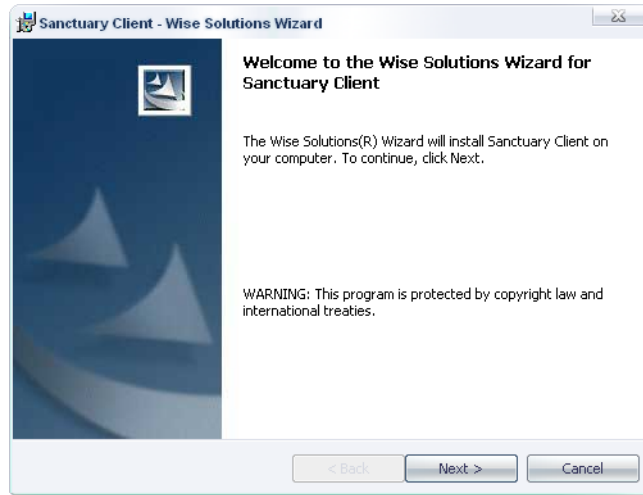
### The Installation Procedure

To install the Sanctuary Client on your MetaFrame Presentation Servers, follow the steps below:

1. Log on to the MetaFrame Presentation Server with administrative rights.
2. Start a command line prompt and type: "**change user /install**", which will change your session from execution to installation mode.
3. Select the "Client" folder on the Sanctuary Application Control Terminal Services Edition CD-ROM or navigate to the network share where the Sanctuary Client setup files are located. Run Setup.exe. The Setup program launches the MSI installer.



When this is complete, the Welcome dialog is displayed. Click on NEXT to continue.



**Figure K.1** Welcome screen

4. The License Agreement is displayed in the next dialog. If you accept the terms of the license agreement, select the *"I accept the terms in the license agreement"* and click *Next* to continue.



- 5. Click *Cancel* to exit without installing your Sanctuary Client.

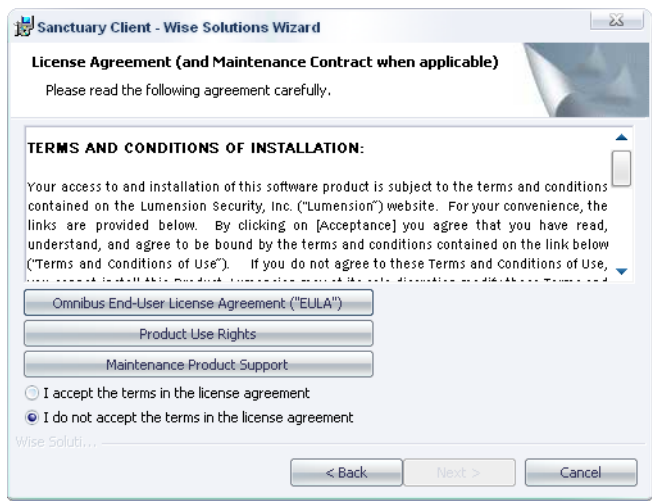


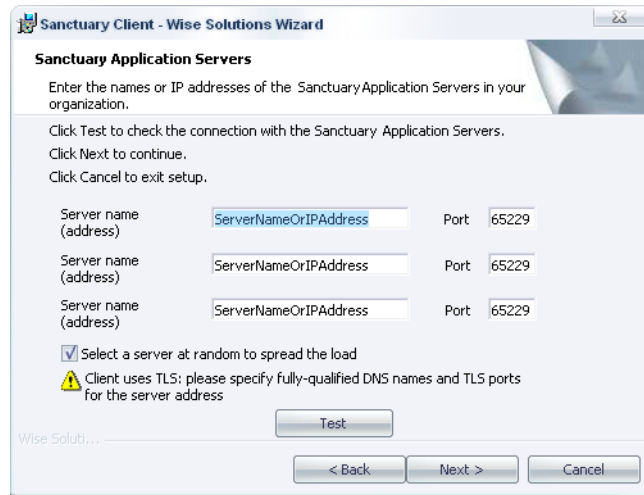
Figure K.2 License agreement

- 6. In the next step, you must decide if the Sanctuary Client use or not TLS protocol to communicate with Sanctuary Application Server (SXS). We recommend selecting TLS protocol (encrypted) — you must already have a valid certificate for the machine. You can use the fist option (non-encrypted communication but still signed with the private key) for testing purposes. Click *Next*.
- 7. Enter the Server name of at least one Sanctuary Application Server on your network. You can enter up to three server names. The dialog accepts fully qualified domain names (FQDN) or IP





addresses. You can also proceed without providing a server address. Do not use IP addresses if you are going to use TLS protocol for communication encryption.



**Figure K.3** Sanctuary Components

8. Click on *Test* to check that the Sanctuary Client can establish a connection with the Sanctuary Application Server(s) listed. A test is considered to be successful if the computer is online and a Sanctuary Application Server could be contacted.
9. By default the driver will choose randomly the available server with which it will work. This setting allows sharing the load between the available Sanctuary Application Servers. If a server is unavailable, then the driver will pick up another one from the list and try to connect to it.
10. You can also choose to contact the servers sequentially in the order you enter them. This setting is particularly adapted to configurations that have a primary Sanctuary Application Server and backup one. The driver will connect preferably to the primary Sanctuary Application Server, the first one in the list. In case it is not available, the driver will try to connect to the next server in the list.
11. Click *Next* to confirm your settings. The server address is verified but you can still continue if it is invalid or unspecified. See details in the *Sanctuary Setup Guide*.
12. In the next step you are prompted for the target directory. You normally will accept the proposed one. Click *Next* button to continue.
13. You can now proceed to select the way the uninstall process is controlled in Windows' *Add or Remove Programs* dialog.

After the final screen, where the actual installation process begins, the Sanctuary Client setup prompts you to reboot one final time.



Once installation is complete, if you do not want to reboot, run "**change user /execute**" in the command prompt window you used at the beginning of the installation.

### Uninstalling the Sanctuary Client

---

At any time after installing Sanctuary Client you can uninstall it from your MetaFrame server. To do this you must log onto the computer using an account with administrative rights.

Since you are now in a highly secure environment, changes to the client (when using the Client Hardening mode) and its components have to be done in an orderly fashion. Even if you are an administrator, the services, registry entries, and special directories of the client cannot be modified before taking some measures to certify that you have the right to do so.

To uninstall the client you should either:

- Deactivate the "Hardening" option using the management console
- Generate an "Endpoint Maintenance Ticket" that overrules the "hardening option"

Please consult the *Sanctuary Application Control Suite User Guide* or the help file for a complete description on how to create an Endpoint Maintenance Ticket.

Select *Add/Remove Programs* from the Windows Control Panel, and choose *Sanctuary Client* from the list of installed programs. The Setup program launches and uninstalls Sanctuary Client. On completion of the uninstall process, you must reboot the server.



# L Installing Sanctuary in Windows XP Embedded

## What is Windows XP Embedded

---

Windows XP Embedded is a componentized version of Windows XP Professional that contains all of the features, functionality, and familiarity of Windows XP Professional. Based on the same binary files as Windows XP Professional, Windows XP Embedded ships with the same set of drivers as the desktop version of Windows XP Professional— that is over 9,000 drivers available as individual components for Windows XP Embedded.

A Windows XP Embedded minimum build size is approximately 5 MB. This is a kernel-only build. An average image size for Windows XP Embedded would be around 40 MB or more. This, of course, is a lot smaller than a typical installation of Windows XP Professional on a desktop. When building the operating system image you can pick and choose which hardware and software components are needed in your platform. E.g. if you do not need Windows Media Player, DCOM, RPC, Microsoft Internet Explorer, then you do not put them in your image.

XP Embedded is marketed towards developers for OEMs, ISVs, and IHVs that want the full Win32 API support of Windows but without the overhead of a full Professional installation. XP Embedded runs existing Windows applications and device drivers on devices with Compact Flash and RAM.

XP Embedded is not related to Windows CE. They target different devices and they each have their pros and cons which make them attractive to different OEMs for different types of devices.

Some of the devices where you can use this system include:

- Thin Clients: Retail Point-of-Sale (POS), Windows-based Terminals.
- Connected Clients: Set-top-boxes, Gateways, Kiosks, ATMs, Industrial Controls, Office Automation, and Gaming Systems.

You can learn more about Windows XP embedded visiting:

<http://msdn.microsoft.com/embedded/>

## Thin Clients

---

A typical thin client configuration application will be to boot and connect directly to a Citrix Server; this is all configured during the creation of the run time image. Typical users never access the thin client the same way as they would do with a “normal” XP Professional Desktop. This is only possible by holding down the SHIFT key at boot, which would display the logon screen.

Windows XP Embedded provides several default shells (Explorer, Command, and Task Manager). The developer can also create a custom shell that offers a specific look for the user interface of the target device, which provides access to the applications and services required for the device, and restricts access to those that are not necessary.



A custom shell is whatever application you want to appear when Microsoft Windows XP Embedded device starts up. Using the custom shell replaces the standard Explorer Shell, Task Manager Shell, or Command Shell. By using your main application as your shell, you can take the user directly to the features you want them to use, and prevent them from switching to nonessential applications, or accessing the control panel or file system.

For example if you are creating a retail point of sale (RPOS) device, you can boot directly into the RPOS application that you or a third-party vendor have created. If you are creating an Internet kiosk, you might boot directly into Internet Explorer by creating and configuring a custom component based on the existing Windows Embedded component for Internet Explorer.

### Available Shells

The Explorer shell component provides support for Windows Explorer. This component configures the operating system to use the Explorer.exe application as the shell application.

The Task Manager Shell component configures the operating system to use the Windows Task Manager as the shell application (to view and/or control applications).

The Command shell component provides support for the command shell. This component configures the system to execute programs, batch files, and scripts displaying their output in the screen. This shell uses Microsoft Windows XP command interpreter, cmd.exe, as the base application.

### What does Windows XP Embedded does not Include

---

Even though Windows XP Embedded is built from the same binary files that Windows XP Professional uses, they do not share all features.

The following Windows XP Professional features are not included in Windows XP Embedded:

- Windows File Protection (WFP): used to prevent system files from being overwritten unless Microsoft digitally signs the files that are being installed. Windows XP Embedded does not enforce system file protection, however, because embedded device users do not typically install software. It is critical for run-time images to be built with the correct versions of system files.
- Windows XP Tour: an interactive, animated tour of the operating system.
- Windows Setup: Windows XP Embedded does not include certain user interface and infrastructure elements.
- Online product activation: Windows XP Embedded-based run-time images are activated by using a run-time product key in the Microsoft Windows Embedded Studio tools.
- Out-Of-Box Experience (OOBE): welcome screens and wizards to help new users set up Internet connections and other operating system features.
- Windows Update: Windows XP Embedded does not use the Windows Update Web site to detect and patch software components.
- System files that support upgrade scenarios
- Obsolete Windows Image Acquisition files



- Microsoft Java Virtual Machine
- Features that are specific to Windows 2000 Server and Windows Server 2003 are also not included in Windows XP Embedded. If an application runs on a Windows Server operating system but does not run on Windows XP Professional, that application will not run on Windows XP Embedded.

## Installing Sanctuary in Windows XP Embedded

---

### What Server Side Components you Need

Before you use Sanctuary Client in a device, you must first install and configure all the other components required to control the Sanctuary Client, notably, the Sanctuary Database, the Sanctuary Application Server, and the administrative tools. Without the first two basic components, you cannot use Sanctuary. Please consult the other chapters of this guide to learn how to install and configure these components.

### What Client Components you Need

In order to install an embedded client, you need to:

1. Create an image
2. Install this image in the device

The first step is done using the Windows Embedded Studio available at Microsoft's Web site. Using this tool, you can generate an image that will then be installed on the target device.

The following tools are included with Windows XP Embedded, as part of the Windows Embedded Studio:

- The Target Designer: provides a development environment to create a bootable runtime image for a target device.
- The Component Designer: is the development tool that enables you to turn your unique application, service, or driver into a component definition that can then be incorporated in the runtime image.
- The Database Manager: facilitates easy management of the component database and the repositories, which are used by the Component Designer and the Target Designer tools.
- The Target Analyzer probe utility: enables automated analysis of the target device, eliminating the need to collect device specific details manually.

Once you have the image, the next step consists on mounting it on the target device. This can be done in one of several ways the most common being using the First Boot agent to complete the installation when first booting the device.

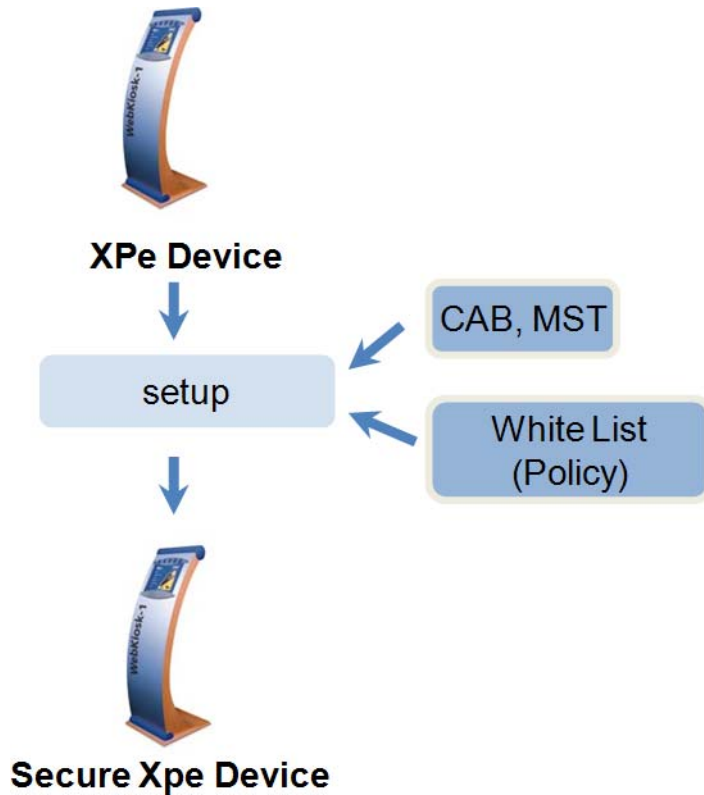
You can learn more about how to "componentize", design run-time images, and creating your final image in Microsoft's Web site.

To install Sanctuary in Windows XP Embedded you have currently two options:

1. Microsoft Software Installer (MSI)



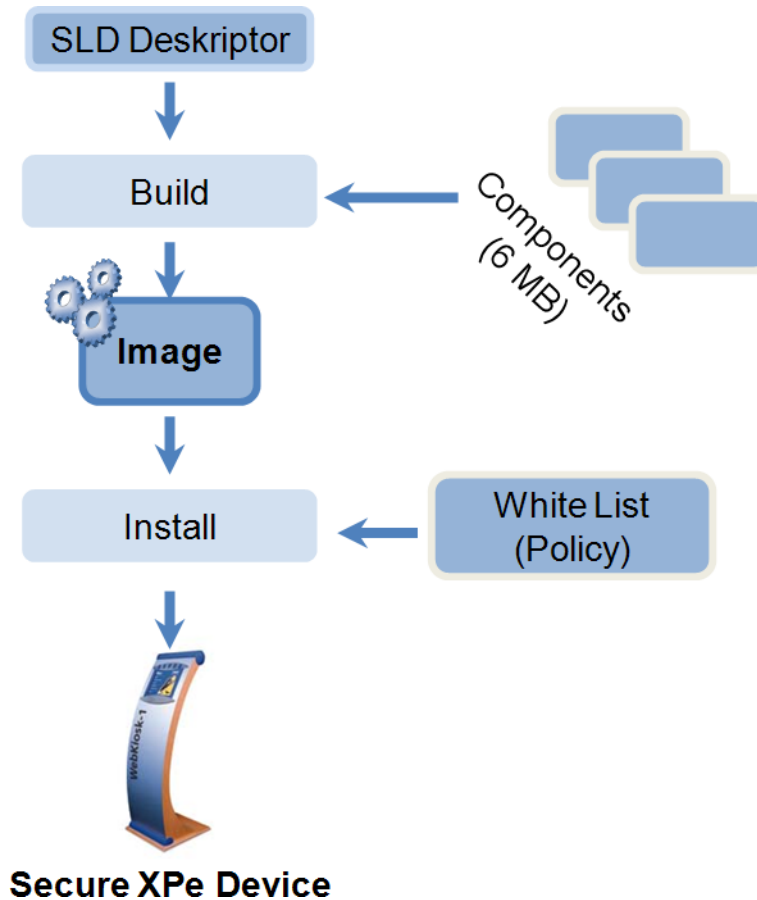
Sanctuary Client is installed the same way as installing any program on Windows XP professional. Windows Installer Service component is available as part of XP embedded OS. See also “[Enhance Write Filter \(EWF\)](#) ” on page 255.



**Figure L.1** Install using MSI (Microsoft Installation file)

### 2. Componentized Application

Componentizing an application is the process of creating one or more custom components that contain the application binaries, resources, and dependencies required by the component that can be included in — or excluded from — a run-time image.



**Figure L.2** Install using SLD (Microsoft Component Definition file) build

## Componentized the Sanctuary Client

The componentized Sanctuary Client created by Lumension is a modular application where the driver functionality is expressed as a set of properties, optional script, and resources, such as files, registry entries, and dependency information.

As embedded device run one or more “custom” applications and/or additional device drivers, you must truly integrate these applications into a device creating components for those applications and including them in your configuration and run-time image.



Components are individually selectable pieces of functionality that can be included in — or excluded from — a run-time image. A component is comprised of properties and resources, such as files, registry entries, and dependency information. The behavior of the component is defined by component script and component DHTML.

A dependency is an additional component required by another one to function properly. Dependencies can either cause the inclusion or exclusion of other components, or control the relative order in which components are included during the run-time image build process. This allows a component to be as small as possible while ensuring that it has all of the resources required to run correctly. A dependency can be expressed upon a single component or upon a group of components known as a dependency group.

For example, if component A requires that component B be built before it, and also requires the presence of component C, the definition of component A must contain a build order dependency upon component B and an include dependency upon component C.

All this data is contained within a .SLD file (File extension for an object definition file).

Functionalities and Devices Supported by Sanctuary in Windows XP Embedded

The next two tables show all functionalities and devices supported when using Sanctuary in Windows XP Embedded:

Table L.1 Functionalities supported by Sanctuary Client

Functionality	Windows XP SP3	Windows XP Embedded
Sanctuary Client Setup	✓	✓
RTNotify		
RTNotify	✓	✓
Sanctuary Management Console Tools Menu		
Synchronize Domain	✓	✓
Send Updates to All Computers	✓	✓
Send Updates to	✓	✓
Purge Online Table	✓	✓
Offline Update		
Offline Update	✓	✓
Reports		
✓ = Supported, X = Not Supported N/A = Not Applicable		





**Table L.1** Functionalities supported by Sanctuary Client

Functionality	Windows XP SP3	Windows XP Embedded
View reports	✓	✓
<b>Sanctuary Device Control Default Options</b>		
Device Control Status Window	✓	✓
Shadow Files Upload Delay or Time	✓	✓
Shadow Directory	✓	✓
Sanctuary Application Server Address	✓	✓
Encrypted Media Key Export	✓	✓
Encrypted Media Export Password	✓	✓
Certification generation	✓	N/A
Centralized Device Control Logging	✓	✓
Suppress recurring log events	✓	✓
<b>Device Explorer</b>		
Default Settings	✓	✓
Manage Devices	✓	✓
Assigning Permissions	✓	✓
Assigning Schedule Permissions	✓	✓
Assigning Temporary Permissions	✓	✓
Assigning Online and Offline Permissions	✓	✓
Shadow	✓	✓
Copy Limit	✓	✓
Computer Group	✓	✓
File Filtering	✓	✓
<b>Media Authorizer</b>		
Media Authorizer	✓	✓
<b>Shadow Files Explorer</b>		
View Shadowed Files	✓	✓
✓ = Supported, X = Not Supported N/A = Not Applicable		



**Table L.1** Functionalities supported by Sanctuary Client

Functionality	Windows XP SP3	Windows XP Embedded
<b>Encrypted communications (TLS protocol)</b>		
Sanctuary Client –Sanctuary Application Server (SXS)and intra SXS-SXS encrypted communications	✓	✓
✓ = Supported, X = Not Supported N/A = Not Applicable		

The following table contains those devices supported by Sanctuary Client running on Windows XP Embedded.

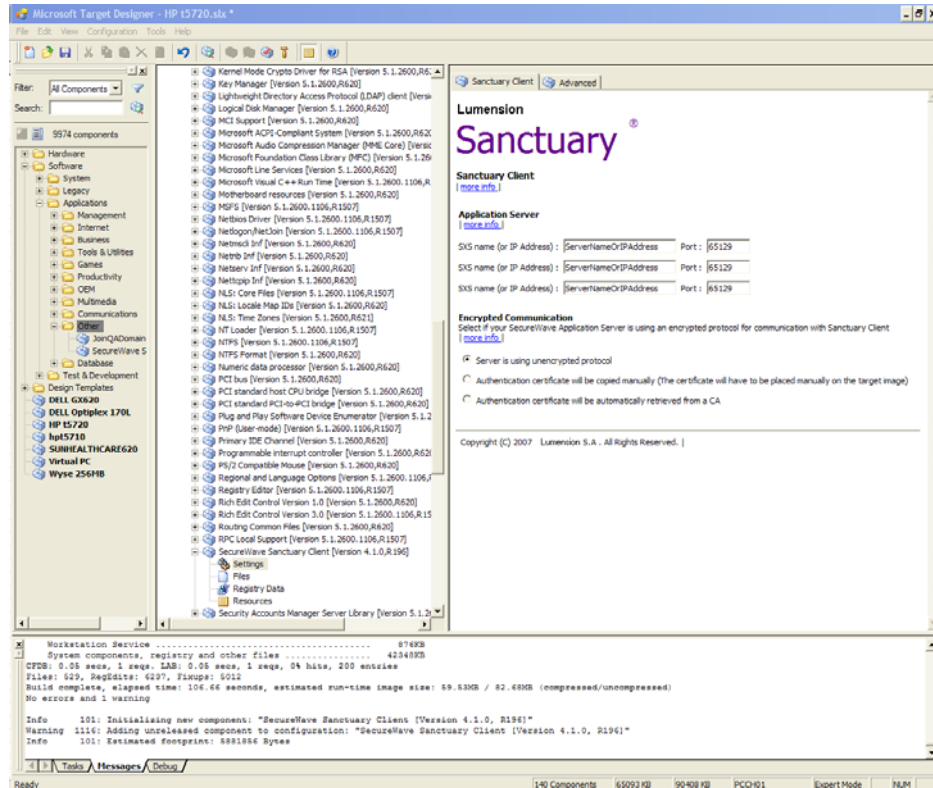
**Table L.2** Device Groups supported by Sanctuary

Device Group	Windows XP SP3	Windows XP Embedded
Biometric Devices	✓	N/D
COM/Serial Ports	✓	N/D
DVD/CD Drives	✓	✓
Floppy Disk Drives	✓	✓
Imaging Devices	✓	N/D
LPT/Parallel Ports	✓	N/D
Modem/Secondary Network Access Devices	✓	N/D
Palm Handheld Devices	✓	N/D
Printers (USB)	✓	N/D
PS/2 Ports	✓	N/A
Removable Storage Devices	✓	✓
RIM Blackberry Handhelds	✓	N/D
Smart Card Readers	✓	N/D
Tape Drives	✓	N/D
User Defined Devices	✓	N/A
Windows CE Handheld Devices	✓	N/D
Wireless NICs	✓	N/A
✓ =Supported, X = Not supported, ND = No Drivers Installed, N/A = Not Applicable		



## How to Configure the Client

While using the Target Designer component of the Windows Embedded Studio you must provide the Sanctuary Application Server IP address or fully qualified domain name as shown on the following image:



**Figure L.3** Configuring the Sanctuary Application Server address or name

## Sanctuary Application Server (SXS)

Sanctuary Application Server (SXS; used to communicate between the Sanctuary Database and the protected clients) should already be installed. To configure a Sanctuary Client, you must provide its IP address or fully qualified domain name in the provided fields. Please refer to the previous figure and section.



### Encrypted Communications

All communications between the Sanctuary Client and the Sanctuary Application Server (SXS) can be fully encrypted if desired. To do this, you will need a valid Certificate Authority installed to issue and manage certificates. If no certificate authority is found, the certificate cannot be issued, or you do not select encrypted communications, the communication channel is still assured by signing messages with a private key.

The Sanctuary Client installation can be done in three distinctive modes:

- ‘Server is using unencrypted protocol’ — No TLS: Communication between Sanctuary Application Server(s) and the Sanctuary Client and is not encrypted but is still signed using the private key. This is, essentially, a legacy communication protocol and not recommended for high security installations.
- ‘Authentication certificate will be copied manually (The certificate will have to be placed manually on the target image)’ — Manual mode using TLS communication: The administrator generates and provides the machine certificate used in all communications. All communication between Sanctuary Client and Sanctuary Application Server(s) is encrypted. This mode is used when there is no Certification Authority installed in the network or cannot be reached when doing the client installation. The machine certificate has to be created by a user (usually the administrator) who already possess a certificate good for issuance and trusted as a root or intermediate Certificate Authority by the Sanctuary Application Server. This authorized user has to be physically present at the machine to create this certificate.
- ‘Authentication certificate will be retrieved form a CA’ — Automatic mode using TLS communication: The program asks for the certificate to one of the selected Certificate Authorities. This certificate must be good for issuance and trusted as a root or intermediate Certificate Authority by the Sanctuary Application Server. All communication between Sanctuary Client and Sanctuary Application Server(s) is encrypted. You do not need a Certificate Authority at this point, but it will be required when first starting the client(s) since the program request a machine certificate. The user who has the rights to create machine’s certificates does not have to be physically present at the machine to do the installation if this mode is selected.

You should ALWAYS use automatic mode when your organization has already deployed a Certificate Authority infrastructure and the Sanctuary servers and clients are part of it. In this case, deployment of Sanctuary Client using TLS is completely transparent and requires no additional action.

Always privilege the automatic mode for issuing valid certificates over all other methods. If it is not possible to use this mode, then you should turn to the manual mode.



**Note:** The semi-automatic mode is not available when installing Sanctuary Client in Windows Embedded machines.

## How to Update Policies

---

If policies are not defined beforehand or, for example, when doing an update or installing another component or software, you will need to update permissions.

Permissions and policies are defined using the Sanctuary Management Console and are sent in two modalities:

1. Online – when all machines are connected through a network or using Internet
2. Offline – when the clients are not connected among them and work as independent units

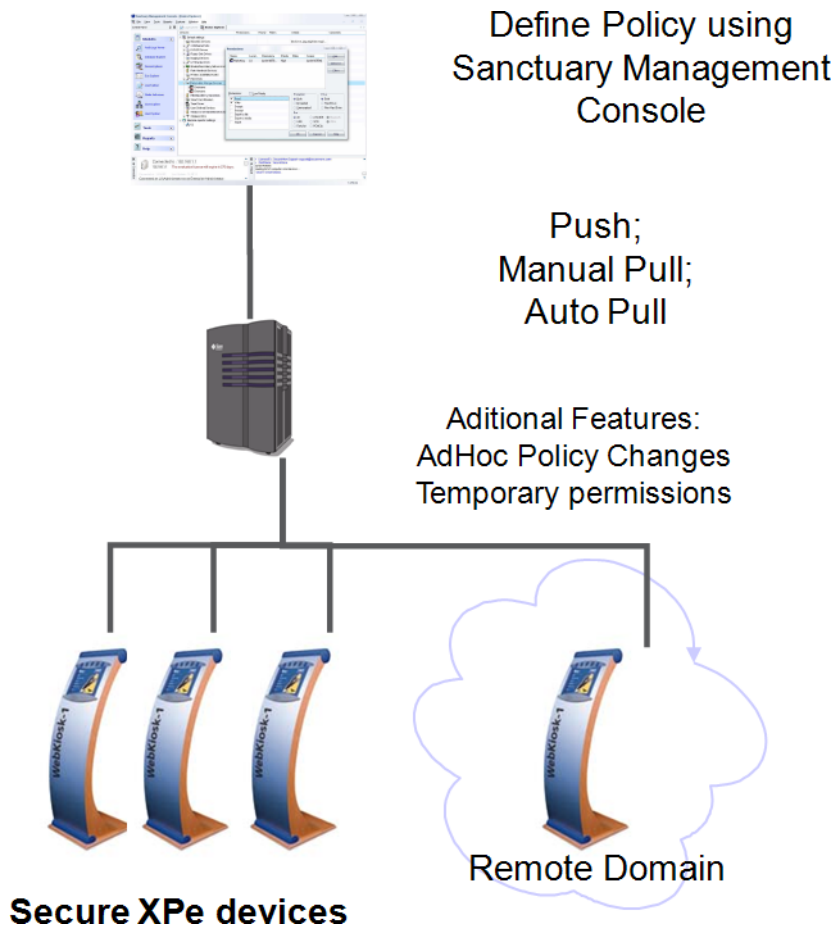
Remember that the Sanctuary Client only communicates to the Sanctuary Application Server. All permissions and rules are stored in the Sanctuary Database.

When doing an online update, policies are defined (using the Sanctuary Management Console) and then sent to all clients in one of three available methods:

- Push – The administrator forces the update using the SEND UPDATES TO command of the management console
- Manual Pull – The client explicitly asks for the updates using the UPDATE command of the right-click menu
- Auto-pull – the client automatically asks for new permissions when the user logs, in a reboot, when the update time defined in the console option is up, etc.

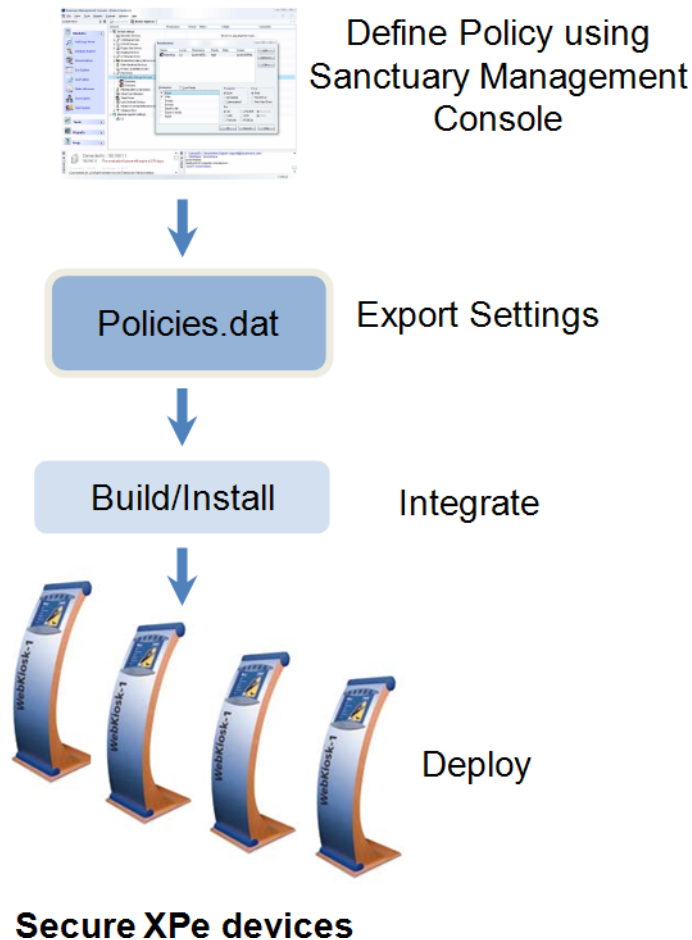


The following image shows how this update is done:



**Figure L.4** Policy update - Online Context (through the network)

When doing an offline update, once policies are defined (new or updated ones) they are exported to a special file (policies.dat) and integrated in the installation/build to be deployed:



**Figure L.5** Policy update – Offline context

## Enhance Write Filter (EWF)

The Enhance Write Filter (EWF) is used to protect one or more disk volumes by intercepting write requests and redirecting them to an overlay volume (RAM or another disk). EWF provides the following functionalities:

- Write protects one or more partitions on your system



- Enables read-only media, such as CD-ROM or flash, to boot and run

There are two major components for EWF:

- EWF Overlay: EWF protects the contents of a volume by redirecting all write operations to an alternative storage location
- EWF Volume: A EWF volume is created on the media in un-partitioned disk space. This EWF volume stores configuration information about all EWF-protected volumes on the device

There are three different modes of EWF based on the different configurations for the EWF overlay and the EWF volume:

- Disk on Disk: used to maintain the state of the system between reboots. The EWF volume is created on disk in an un-partitioned space.
- RAM in RAM: utilized to discards any write information after reboot or to delay writing the overlay to the media. The EWF volume is created on disk in an un-partitioned space.
- RAM Reg in RAM: similar to EWF RAM types, RAM Reg overlays stores information in RAM. However, the configuration information about EWF is not stored in a separate EWF volume, but within the registry.

### Sanctuary Client & EWF

Enhanced Write Filter needs to be disabled prior to installing Sanctuary Client and re-enabled afterwards. If you fail to do this, no changes will be written to the disk volume, and the disk volume will be reverted back to its previous state after rebooting the machine.

The client running with EWF enabled is able to pick up all permissions from the server after a reboot, including managed devices and temporary permission.

You can activate/deactivate Enhance Writer Filter from within the Control Panel.

### Minimum Requirements

---

The following list specifies the minimum system requirements needed for a **Microsoft Software Installer** installation of Sanctuary Client on XP Embedded Thin Clients:

- Flash Memory: Minimum 256 MB
- RAM: Minimum 256 MB
- Additional Free Space: Minimum 10 MB
- Component Required: Microsoft Software Installer

### Known Issues

---

The following issues have been encountered when installing Sanctuary in Windows Embedded:

- The user notification is only displayed in the Explorer Shell
- The Rtnotify icon is only displayed in the Explorer Shell





- The RTNotify icon is displayed only when the “Show notification in Taskbar” setting is selected within the user interface core component
- Any changes to default settings of the client install would require to disable EWF
- If the Sanctuary Application Server (SXS ) is unavailable, permissions acquired on initial installation of client are applied
- As XP embedded is used for building custom Operating Systems, even if Microsoft Installer Service is available as part of the run time images, other components may not be present for Sanctuary Client to run correctly. For this reason, Lumension also provides a componentized application.
- You cannot deploy Sanctuary Client on XP Embedded Thin Clients using deploy.exe
- The public file key — sx-public.key — import is currently not possible using the componentized application. This deployment has to be done manually into the %SystemRoot%\sxdta directory. This can be done by copying this file into your run-time image before deploying it.
- The Sanctuary Application Server (SXS ) has to be up and running when your client boots so that it can retrieve the initial permissions. You will also need to start the client machine with the Enhanced Write Filter (EWF) disabled so that the default permissions are kept. You can enable EWF once the client machine has started.





# M

## Glossary

### ACE

*Access Control Entries.* An entry in the Access Control List (ACL) that contains a set of access rights and a security identifier (SID) identifying a trustee.

### ACL

*Access Control List.* A list of security protections that apply to an object (file, process, event, or anything else having a security descriptor).

### ADC

Advanced Data Connector. See RDC.

### ADSI

Acronym for *Active Directory Service Interface*. Previously known as OLE Directory Services, ADSI makes it easy to create directory management applications using high-level tools such as Java, or C/C++ without having to worry about the underlying differences between the dissimilar namespaces.

### AES

*Advanced Encryption Standard.* A symmetric key encryption technique that is replacing the commonly used DES standard. It is the result of a worldwide call for submissions of encryption algorithms issued by NIST in 1997 and completed in 2000.

### CAB

File extension for cabinet files, which are multiple files LZx-compressed into a single file and extractable with the extract.exe utility. Such files are frequently found in Microsoft software distribution packages.

### Certificate Authority (CA)

Authority charged of issuing user or computer certificates (among other tasks).

### Certificate store

The storage location where Windows locally saves certificates requested by a computer or device. This store can have several certificates possibly issued by various CAs. If you have the user rights to do so, you can import or export certificates from any folder or file to the certificate store.

### Certificate revocation list (CRL)

A list containing the compromised, revoked, or superseded certificates. The CRL is used during the digital signature verification process to certificate's validity using the public key extracted from the same certificate.

### Client Computer

The computers on your network that Sanctuary Application Control Suite and Sanctuary Device Control protects/controls.



### Component

Smallest individually-selectable piece of functionality that can be included in or excluded from a run-time image. A component is comprised of properties and resources, such as files, registry entries, and dependency information. The behavior of the component is defined by component script and component DHTML. Applies to Windows Embedded.

### Component definition

The Component Definition forms the data that constitutes a particular component, including information about component script, resources (files and registry keys), and dependencies. The definition is saved in an .sld file so it can be imported into the component database. Applies to Windows Embedded.

### Delegation

The act of assign responsibilities for management and administration of a portion of the resources or items used in a shared computing environment to another user, group, or organization.

### Dependencies

Additional executable files (.exe, .dll, or others) required by executable files to run properly.

Dependencies are split into two categories: *static dependencies* — that are files declared explicitly in the executable file as being required, and *dynamic dependencies* — which are additional files an executable may require at runtime.

### Direct cable connection (DCC)

A RAS networking connection between two computers, or between a computer and a Windows CE/PPC-based device, which uses a serial or parallel cable directly connected between the systems instead of a modem and a phone line.

### DN

*Distinguish Name*. A name that uniquely identifies an object in the Directory Information Tree.

### DNS

*Domain Name System* (also *Service or Server*). A service that translates computer names into IP addresses.

### Embedded

Software code or commands built into a device, as opposed to software that is added. In a narrower sense, code that is typically stored in ROM and dedicated to either controlling a device or providing a specific functionality.

### Enhanced Write Filter (EWF)

Tool that protects underlying media or partitions from write operations, thus rendering the media read-only. Write operations to the media are diverted to a secondary storage location. Applies to Windows Embedded.



## Executable Program

A computer program that is ready to run. The term usually applies to a compiled program translated into computer code in a format that can be loaded in memory and executed by a computer's processor.

## Exploit

A piece of software that takes advantage of a bug, glitch or vulnerability, leading to privilege escalation (exploit a bug) or denial of service (loss of user's services) on a computer system.

## FAT

*File Allocation Table*. This defines a reserved zone on a magnetic media containing the list of clusters it occupies.

## File Group

Organizational groups used to cluster authorized executable files. Files must be assigned to File Groups before users can be granted permission to use them. You can choose to assign files to File Groups using several Sanctuary Management Console modules (*Database Explorer*, *Explorer*, *Log Explorer* and *Scan Explorer*).

## Hash

A complex digital signature calculated by the Sanctuary Application Control Suite components to uniquely identify each executable file, script or macro that can be run. The hash is calculated using the SHA-1 algorithm that takes into account the entire contents of the file.

## IOCP

**I/O Completion Port**.

## MDAC

*Microsoft Data Access Components*. This is required by Windows computers to connect to SQL Server and MSDE databases.

## MSI

*Microsoft's Windows Installer* engine (Sanctuary supports MSI version 3.1). It is also the extension of the file used by this component. An MSI file is basically a database with relationally linked tables and a set of files either inside or accompanying the MSI file. This database contains information about what has to be done to the target machine in order to install the application.

## NAT

*Network Address Translation*. A technique of trans-receiving network traffic through a router and rewriting the source and/or destination IP address as they pass through. This is done so that multiple host on private networks can access a single public IP address.

## NTFS

*New Technology File System* offers several enhancements and advantages over older FAT systems. These include an improved architecture, support for larger files, enhanced reliability, automatic encryption/decryption, change journals, disk defragmenter, sparse file support, improved security and permissions, etc.



### Private Key

One of two keys used in public key encryption. The user keeps the private key secret and uses it to encrypt digital signatures and to decrypt received messages.

### Public Key

One of two keys in public key encryption. The user releases this key to the public, who can use it for encrypting messages to be sent to the user and for decrypting the user's digital signature.

### RAS

*Remote Access Services* is a Windows program that allows most of the available network facilities to be accessed over a modem link.

### RDC

*Remote Data Connector*. Formerly known as *Advanced Data Connector*. Technology used in conjunction with ActiveX Data Objects (ADO) to retrieve a set of data from a database server.

### RPC

*Remote Procedure Call*. A protocol that allows a computer program running on one host to run a subroutine located on another one. RPC is used to implement the client-server model of distributed computing.

### Sanctuary Application Server (SXS)

The Sanctuary component that serves as a link between Sanctuary Client and the Sanctuary Database

### Sanctuary Management Console (SMC)

The console used to define the device permissions and default options. Its functions are described in the corresponding User Guide.

### SCC

*Sanctuary Command & Control*. The Sanctuary component that is in charge of all communication between server and client(s). It also communicates with the CA (Certificate Authority) Server.

### SFD

*Standard File Definitions*. Lumension provides a number of pre-computed file hashes for most versions of Windows Operating Systems, in several languages, and for all the available Service Packs. These are typically installed during setup, but you can also import new ones.

### SID

*Security Identifier*. This is a unique alphanumeric character string. It identifies each operating system and user in a network.

### SMC

See Sanctuary Management Console.



## SQL Server

The industry standard database server, supported by Sanctuary. Either MSSQL 2000 SP4, MSSQL 2005 SP2, or SQL Server 2005 Express Edition SP2, can be used with Sanctuary.

## SK

The Sanctuary Kernel Driver, the client component that runs as a kernel driver.

## SUS

*Software Update Services* is a tool provided by Microsoft to assist Windows administrators with the distribution of security fixes and critical update releases.

## SXS

See *Sanctuary Application Server*.

## TCP/IP

*Transmission Control Protocol/Internet Protocol*. The protocol used by the client computers to communicate with the Sanctuary Application Server.

## TLS

*Transport Layer Security*. The protocol (based on SSL — Secure Socket Layers) that addresses security issues related to message interception during communication between hosts.

## UAC

*User Account Control*. A new security component used in Windows Vista that enables users to perform common tasks as non-administrators, called standard users, and as administrators without having to switch users, log off, or use the Run As command.

## UPC

*Universal/Uniform Naming Convention*. A path convention that uses a \\server\volume\directory\file convention instead of arbitrary mapped letters to describe the actual location of a file or directory.

## Well-Known Security Identifiers

A security identifier (SID) is a unique value used to identify a security principal or security group. The values of certain SIDs remain constant across all installations of Windows systems and for this reason are termed well-known SIDs. Everybody, Local, Guest, Domain Guest, etc. are some examples of such SIDs.

## WINS

*Windows Internet Naming Service* (formerly known as WBEM). A system that determines the IP address associated with a particular network computer (called name resolution). WINS uses a distributed database that is automatically updated with the names of computers currently available and IP addresses assigned to them.



### **WMI**

*Windows Management Instrumentation*. WMI is a set of extensions that provide an operating system management technology allowing scripts to monitor and control managed resources throughout the network.

### **WSUS**

*Windows Server Update Services* (previously SUS v2.0) is a new version of Software Update Services (SUS).

### **.sld file**

File extension for an object definition file. Applies to Windows Embedded.





# N Index

## Symbols

..... 17

## A

ACE ..... 259  
 ACL ..... 259  
 Active directory .... 203, 204, 209, 214  
 Active Directory Service Interface 259  
 ADC ..... 259  
 Administration tools ..... 1  
 ADO ..... 175  
 ADSI ..... 259  
 Advanced Encryption Standard .... 259  
 AES ..... 259  
 Anonymous access ..... 176  
 Architecture ..... 1  
 AuthSrv.exe ..... 85  
 Automatic Load Balancing ..... 102

## B

Basic Security Rules ..... 13  
     Access policy ..... 15, 16  
     Administrative rights ..... 14  
     BIOS password ..... 14  
     Boot sequence ..... 13  
     Firewalls ..... 16  
     Hot fixes ..... 15  
     NTFS partition ..... 15  
     Password policies ..... 16  
     Power users ..... 15  
     Private and public key generation 16  
     Recovery console ..... 15  
     Safe mode ..... 15  
     Seal/chassis intrusion protection 14

Service packs ..... 15

## C

CA ..... 259  
 CAB ..... 259  
 CD/DVD burning ..... 13  
 Certificate authority ..... 259  
 Certificate revocation list ..... 259  
 Certificate store ..... 259  
 Certificates 7, 210, 211, 212, 213, 214  
     Installing ..... 204  
     Requirements ..... 203  
     Services ..... 204  
     Verifying ..... 210, 214  
 Checklist  
     see installation checklist  
 Client  
     Components ..... 245  
     Configuration ..... 251, 253  
 Client computer 32, 113, 117, 124, 259  
 Cluster ..... 25, 42  
 Clustering ..... 24  
     Definition ..... 24  
     Implementation ..... 26  
     Majority node set ..... 26  
     Requirements ..... 25  
     Single node server ..... 26  
     Single quorum ..... 26  
     Terminology ..... 25  
 Command-line ..... 117  
 Component ..... 260  
 Component definition ..... 260  
 Componentized the Sanctuary Client ..  
     247



Computers menu .....	126	EWf .....	255, 260
CRL .....	259	Executable	
ctrlacx.vbs .....	215	Files .....	260
Configuration steps .....	217	Executable program .....	261
Examples .....	216	Exploit .....	261
Requirements .....	215	Export .....	127
Usage .....	216		
<b>D</b>		<b>F</b>	
Data File Directory .....	1, 42	Failback .....	25
data reception .....	154	Failover .....	25
Database .....	3, 17, 18, 33, 133, 142	FAT .....	261
Choosing .....	17	File groups .....	261
Engine .....	17, 19	Firewall .....	175, 179
DataFileDirectory .....	42	Ports .....	181
Delegation .....	260	Fixed Endpoints .....	177
Dependencies .....	260		
Deploy Software .....	122	<b>G</b>	
Deployment package .....	95, 125	Generating a Key Pair .....	30
DFD .....	1, 42	Ghost .....	62
Direct cable connection .....	260	Ghost images .....	5
DN .....	260	GrantDB.exe .....	35
DNS .....	203, 260	Group Policy .....	118
DriveImage .....	62		
<b>E</b>		<b>H</b>	
edrDspPauseFail .....	155	Hardening option .....	80, 242
Embedded .....	260	Hash .....	261
EnableAuthEpResolution .....	177	Heartbeat .....	25
Encrypted Communications .....	252	Help menu .....	128
Endpoint Maintenance Ticket ...	80, 96, 101, 127, 242		
Enhance Write Filter .....	255	<b>I</b>	
Sanctuary Client .....	256	IMAPI .....	13
Enterprise Manager .....	35	Import .....	125, 127
		Install/Uninstall/Reboot Options dialog	113, 117
		Installation Transform .....	100



Installing .....	1	<b>N</b>	
Sanctuary Management Console	53	nscan_ip_tcp .....	177
Installing a Certificate Authority...	203	Node .....	25
Instance .....	41, 42	Novell .....	187
IOCP .....	261	Components .....	187
<b>K</b>		FAQ .....	190
Key pair .....	29, 30, 31, 224	Interface .....	188
Generation .....	29	Synchronization script .....	187
Mismatch .....	103	NTFS .....	261
Known issues .....	256	NTLM .....	178
<b>L</b>		<b>O</b>	
License .....	39	Open last log .....	127
File format .....	142	Options .....	130
File location .....	142	Installation Transform .....	97
Log		Organizational Unit .....	119
To file .....	156	Overview .....	1
Log insertion process .....	154	<b>P</b>	
Lumension Security		Package .....	95, 97, 99, 106, 111, 116, 122, 124, 125
contacting .....	xiv–xvi	Colors .....	106
<b>M</b>		Warning .....	106
Maximum number of nodes .....	25	Packages	
MDAC .....	34, 148, 175, 261	Menu .....	99
Microsoft Certificate Authority .....	150	Packages menu .....	124
Minimum requirements .....	256	policies.dat .....	63, 101
MSCS .....	25	Port .....	175
MSDE .....	17, 18, 261	Power users .....	15
MSI files .....	95, 97, 99, 261	pricing	
MsiExec .....	117	product .....	xv
MST file .....	105	Private Key .....	262
MST files .....	95, 97	product	
		pricing .....	xv
		Progress details .....	127
		Public key .....	106, 125, 262



**Q**

Query ..... 124, 127  
Quorum..... 25

**R**

RAS ..... 262  
RDC..... 262  
Reboot ..... 113, 117, 127  
Registering Sanctuary ..... 141  
Registry  
    AdoVersion ..... 156  
    CertGeneration..... 163  
    CertificateQueryPeriod..... 157  
    Classes..... 165  
    CommVer ..... 157  
    ComputerName ..... 165  
    Concurrency..... 156  
    Data File Directory ..... 157  
    DbConnectionCount ..... 153  
    DbConnectionMaxCount..... 153  
    DbConnectionPoolTimeout..... 153  
    DbConnectionString ..... 154  
    DbLossLatency ..... 154  
    DbPingPeriod..... 154  
    Debug..... 155, 163, 165  
    edrBatMaxDuration ..... 154  
    edrBatMinEntries ..... 154  
    edrDspPause ..... 154  
    edrDspRetryCount ..... 155  
    edrDspThreads ..... 155  
    edrQueLength ..... 155  
    edrStaPeriod ..... 155  
    edrTmpTimeout ..... 155  
    Enum ..... 165  
    EventLog ..... 165  
    EventMessageFile ..... 162  
    FileLog ..... 165  
    FirstServer..... 163  
    ForceLCID..... 166

HardeningMode ..... 164  
HardeningStatus ..... 164  
HID..... 164  
HistoryPeriodSecs ..... 164, 165  
ImportDir ..... 164  
IpaqDetectDelay ..... 164  
LastSeenComputerName..... 164  
LastSxLogUploadTime..... 164  
Limits ..... 165  
Log file name ..... 155, 164  
Log to console ..... 155, 164  
Log to dbwin ..... 155, 164  
Log to file ..... 155, 164  
LogMonitorDlls..... 155  
LogMonitorPeriod ..... 156  
LogMonitorResetOptions ..... 156  
LogMonitorThreshold ..... 156  
MaxSockets..... 158  
OnLineMonitorPeriod ..... 157  
OnLineStateExpiry ..... 157  
Port ..... 158  
Products ..... 157  
ReportGenerationTimeout ..... 162  
ReportMaxRecords ..... 162  
ReportStoragePath..... 163  
ReportThreads..... 162  
RpcProtectionLevel..... 158  
Salt..... 164  
SecureInterSxs..... 159  
Security..... 165  
Servers ..... 164  
ServersOverride..... 164  
ShadowDirHistory ..... 164, 165  
SndPort ..... 159  
SxdConnectTimeoutMSec ..... 159  
SxdPort ..... 159  
TicketDir..... 164  
TLSMaxSockets ..... 159  
TLSPort ..... 159  
TypesSupported..... 163  
UseTLS..... 165



VerboseSyncLogging .....	156	SHA-1 .....	261
Registry Keys .....	153	SID .....	259, 262
Remove .....	126	SK .....	263
RestrictRemoteClients .....	176	SLD file .....	264
RPC .....	175, 262	SMC .....	262
RunAs .....	152	SQL Server .17, 18, 34, 154, 261, 263	
<b>S</b>		SSL .....	6
Sanctuary		Support	
Common requirements .....	150	contacting Lumension Support ..xvi	
Supported devices .....	248	Supported functionalities .....	248
Sanctuary Administration Tools		SUS .....	85, 263
System requirements .....	148	sx database .....	20
Sanctuary Application Server1, 33, 262		SXDomain .....	xi, 133
Registry keys .....	153	SXS .....	262, 263
Sanctuary Authorization Service Tool85		Synchronize Domain Members .....	156
Sanctuary Client .....	xi, 1	System	
Deployment .....	106	Requirements .....	61
Installation .....	238	Shutdown dialog .....	117
Installing .....	61	System Requirements .147, 153, 167,	
Registry keys .....	163	175, 181, 187, 195, 203, 215,	
System requirements .....	149	221, 243	
Uninstall .....	242	<b>T</b>	
Sanctuary Client Deployment Tool 106		TCP .....	175
Sanctuary Database .....	1, 17	TCP/IP .....	34, 263
System requirements .....	148	TDS .....	175
Sanctuary Management Console .....	3	Terminal Services .....	151
SCC .....	262	Limitations .....	151
Sanctuary Command Control ..	262	Testing .....	33, 133, 141
Scheduling domain Synchronizations ..	135	The RunAs command limitation ....	152
Select computers .....	111, 114	Ticket .....	80, 242
Serverless mode .....	101	TLS .....	6, 10, 252, 263
Server-side .....	1	Transform files .....	95
SFD .....	262	Transport Layer Security .....	263
Standard File Definitions .....	262	Troubleshooting .....	147



U

UAC ..... 64, 263

Unattended ..... 79, 93

Uninstalling ..... 79

UPC ..... 263

Upgrade ..... 169, 170

Using the Key Pair Generator ..... 29

V

VIP ..... 25

Virtual IP ..... 25

VirtualServerName ..... 42

W

Well-known

    Security Identifiers ..... 263

Windows 2003 SP1 ..... 175

Windows Authentication ..... 35

Windows Installer ..... 261

Windows XP Embedded ..... 243

    Client components ..... 245

    Installing ..... 245

    Shells ..... 244

    Thin clients ..... 243

    Uses ..... 243

Windows XP SP2 ..... 175

WINS ..... 263

WMI ..... 264

WSUS ..... xi, 85, 264







**Lumension Security**

15880 North Greenway Hayden Loop,  
Suite 100  
Scottsdale, AZ 85260

[www.lumension.com](http://www.lumension.com)  
phone: 480.970.1025  
fax: 480.970.6323

